Security Guide

Leitfaden für Unternehmen und Professionals
inklusive Security Update

Sichere Cloud-Systeme &
Security Management

Digitale Identitäten &
Mobile Security

Cybercrime, Schadsoftware &
Erste Hilfe

Forschung &
Security-Ausbildung in Österreich

inklusive
A-SIT
Checkliste zur
Passwort-
Sicherheit

A-SIT

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

TU Graz

BRZ

DONAU UNIVERSITÄT KREMS

JKU
JOHANNES KEPLER
UNIVERSITÄT LINZ

„DIGITALISIERUNG
ist zum einen JOB-MOTOR
und zum anderen TREIBER
für VERÄNDERUNGEN.
Hier braucht es den
SCHULTERSCHLUSS zwischen
der gesamten Öffentlichen Verwaltung,
Wirtschaft und der Gesellschaft.“

Mag.ª Maria Ulmer, BMDW

Cyber-Security im Schnittfeld von Innovation, Wissenschaft und Praxis stellt uns laufend vor neue Herausforderungen. Durch ein abgestimmtes Vorgehen zwischen Privatwirtschaft und öffentlicher Verwaltung leistet A-SIT als gemeinnützige Einrichtung seinen Beitrag und stimmt diesen auch international und auf der EU-Ebene ab."

Prof. Dr. Reinhard Posch

Impressum:

Medieninhaber und Verleger: MediaGuide GmbH, A-1150 Wien, Pillergasse 13, Tel: 0664/100 39 06, Fax: +43/1/897 48 60-22
Herausgeber: Zentrum für sichere Informationstechnologie – Austria (A-SIT)
Chefredaktion: Dipl.-Ing. Dipl.-Ing. Gerald Dißauer, Tel: +43/1/503 19 63 - 0, gerald.dissauer@a-sit.at; www.a-sit.at
Grafik: Agentur be-design, Karin Schön, office@be-design.at, www.be-design.at
Fotos: ©AdobeStock, Archiv und Vertragspartner
Druck: Kny und Partner, office@knyundpartner.com

Das Medium Cyber-Security-Guide erscheint durch das Zentrum für sichere Informationstechnologie – Austria (A-SIT) im März 2021. Dennoch erfolgen alle Angaben mit dem Status März 2021 ohne Gewähr. Der vorliegende Guide wurde von Fachleuten sowie von Expertinnen und Experten begutachtet und für gut befunden. Dennoch erfolgen alle Angaben ohne Gewähr. Weder die Autorinnen oder Autoren bzw. die Expertinnen oder die Experten, noch der Verlag können für eventuelle Nachteile oder Schäden, die aus den im Heft gegebenen Hinweisen resultieren, eine Haftung übernehmen. Veröffentlichung oder teilweise Veröffentlichung nur mit schriftlicher Genehmigung des Verlages. Anzeigenannahme: Falls Sie mehr über die Kooperationsmöglichkeiten im Cyber-Security-Guide wissen möchten, fordern Sie bitte nähere Informationen:
MediaGuide Verlag Tel. 0664/100 39 06, E-Mail: angermayr@myguides.at
Herzlichen Dank an alle, die zur Vollständigkeit und zum Gelingen durch ihre engagierte Mitarbeit beigetragen haben.

Sicherheit sollte direkt in die Digitalisierung eingebaut werden

Die aktuelle Situation verdeutlicht den Mehrwert der Digitalisierung: Der Fokus auf deren Ausbau in Wirtschaft und Verwaltung hat in den letzten Jahren Österreich sehr positiv beeinflusst. Ein Gebot der Stunde ist, die dafür notwendige Modernisierung konsequent voranzutreiben, damit der Fortgang dieses Prozesses nicht nur halbherzig geschieht. So wurde bereits im Jahr 2019 der Digitale Aktionsplan Austria zur Schaffung einer „Digitalen Verantwortungsgesellschaft" ins Leben gerufen, der sich verstärkt mit dem Thema Wachstum und Innovation auseinandersetzt. Nun ist der Aspekt der Krisenfestigkeit dazu getreten.

Sicherheit im Netz ist dabei immer ein Thema, etwa in der Form sicherer elektronischer Identitäten wie das österreichische Best Practice, die Handy-Signatur, eindrucksvoll zeigt: Über 1,7 Millionen Österreicherinnen und Österreicher nutzen diese tragende Säule elektronischer Identitäten bereits, um Amtswege bequem online zu erledigen oder um Dokumente in rechtssicherer Form digital zu signieren.

Digitalisierung muss immer auf den leistungsfähigen Beinen von sicheren IT-Systemen stehen. Vor diesem Hintergrund wurde von öffentlicher Seite im Jahr 1999 das Zentrum für sichere Informationstechnologie – Austria (A-SIT) als Verein gegründet. A-SIT wird privatwirtschaftlich als kompetentes Zentrum für IT-Sicherheit geführt. Das Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW) ist Mitglied des Vereins und repräsentiert den gesamten Bund. Ebenso Mitglied sind die Technische Universität Graz, das Bundesrechenzentrum, die Donau-Universität Krems und die Johannes Kepler Universität Linz. Die Aktivitäten decken vor allem drei große Bereiche der Cy-

> „Österreich soll sich zu einem digitalen Security-Leader entwickeln, um Sicherheit direkt in die Digitalisierung einzubauen und damit tausende Jobs zu schaffen."

1,7 M

aktivierte Handy-Signaturen, um Amtswege bequem online zu erledigen oder um Dokumente in rechtssicherer Form digital zu signieren

1999

von öffentlicher Seite gegründet, wird A-SIT privatwirtschaftlich als kompetentes Zentrum für IT-Sicherheit geführt

40

Kooperationspartner aus der öffentlichen Verwaltung und der Wirtschaft betreuen gemeinsam mit A-SIT das IKT-Sicherheitsportal www.onlinesicherheit.gv.at

ber-Security ab: Erstens Bestätigungen bzw. Konformitätsbewertungen, Begutachtungen und Evaluierungen, im Weiteren Forschung und Technologiebeobachtung sowie darüber hinaus innovative Anwendungsunterstützung.
Seit 2013 betreut A-SIT auch das IKT-Sicherheitsportal www.onlinesicherheit.gv.at, einen Schulterschluss zwischen öffentlicher Verwaltung und der Wirtschaft mit circa 40 Kooperationspartnern. Das vom BMDW betriebene Portal beschäftigt sich mit Themen rund um die Sicherheit in der digitalen Welt und informiert sowohl Anwenderinnen beziehungsweise Anwender als auch Profis über Gefahren und Entwicklungen im IT-Bereich.
Der vorliegende Band zeigt die aktuellen Schwerpunkte in der Onlinesicherheit: Hierzu zählen vordergründig die Cloud-Technologie, ID Austria und eIDAS für elektronische Identitäten sowie wegweisende Security-Forschung und entsprechende Ausbildungen am Wirtschafts- bzw. Digitalisierungsstandort Österreich. Dazu wünsche ich allen Leserinnen und Lesern mit dieser Broschüre viele neue Erkenntnisse und praktische Anregungen für eine verbesserte Sicherheit im Netz.

Mag. Wolfgang Ebner
BMDW, Präsident A-SIT

„Zukunftsweisende Security-Ausbildung für den Standort Österreich

Der Wandel durch die Digitalisierung führt zu komplexeren, hochgradig verteilten IT-Systemen. Daraus ergeben sich Chancen zur Wertschöpfung. Gleichzeitig sind damit auch Risiken verbunden. Cyberattacken und Cyberkriminalität sind immer häufiger zu beobachtende Phänomene. Vor diesem Hintergrund sollte risikobasiert ein hohes Sicherheitsniveau gleich von Beginn an in IT-Systeme integriert werden. Leider hakt es in diesem Zusammenhang oft beim Bewusstsein.

Die Initiative GEMEINSAM.SICHER fIT im Netz hilft, das Bewusstsein für die Herausforderungen der IT-Security zu stärken. Auch brauchen wir eine einheitliche IT-Bildungsstrategie für Universitäten, Fachhochschulen, berufsbildende Schulen und die Lehre. In Europa herrscht ein Mangel von etwa 1.000.000 IT-Expertinnen und Experten – eine besorgniserregende Beobachtung. Auch in Österreich kommen vor diesem Hintergrund Institutionen, Unternehmen sowie Organisationen vermehrt in Bedrängnis. Wie die Studie „IT-Qualifikationen für die österreichische Wirtschaft“, die wir in enger Kooperation mit dem Fachverband für Elektro- und Elektronikindustrie (EEI) sowie mit der Metalltechnischen Industrie (MTI) verfasst haben belegt, fehlen in Österreich gut 24.000 IT-Fachkräfte – Tendenz steigend. Diese unbesetzbaren Stellen kosten dem Wirtschaftsstandort Österreich umgerechnet 3,8 Milliarden Euro pro Jahr. Zusammen mit A-SIT und weiteren Partnerorganisationen wie etwa dem KSÖ haben wir den anerkannten Incite-Lehrgang „Data & IT Security“ ins Leben gerufen. Durch die langjährige Partnerschaft mit A-SIT bringen wir gemeinsam IT-Sicherheit auf den Boden.

Dass bereits 51% der Unternehmen die hohe Qualität der IT-Ausbildung in Österreich bestätigen, ist eine gute Ausgangslage. Wir dürfen aber keinesfalls nachlassen und sollten in den nächsten Gang schalten. Nur so kann sich Österreich zu einem digitalen Security-Leader entwickeln. Dafür braucht es nationale, aber auch internationale Kooperationen. Heute wissen wir, dass IT-Sicherheit eine

1,0 M

fehlende IT-Expert/innen
in ganz Europa

24.000

fehlende IT-Fachkräfte
in der Österreichischen Wirtschaft

51%

der Unternehmen stimmen der hohen
Qualität der IT-Ausbildung in Österreich zu

tragende Säule der Digitalisierung ist. Überdies steuern in diesem Themenfeld innovative Geschäftsmodelle in den Bereichen der Privatsphäre sowie der IT-Sicherheit große Wertschöpfungspotentiale bei. Damit können wir wertvolle Jobs schaffen und unseren Wirtschaftsstandort stärken.
Erfolgreiche Lösungen aus Österreich wie etwa die Handy-Signatur, stärken die Rechtssicherheit im digitalen Raum. Solche Innovationen sind ohne treffsichere Beratungsleistungen in Verbindung mit Spitzenausbildung und Zusammenarbeit nicht erreichbar. Auch wird die Beratung in den Themenfeldern Cyber-Security, Datenschutz und Digitalisierung für eine solide Datensouveränität immer wichtiger.

Es gilt, rechtzeitig etwas zu tun und unsere Anstrengungen zu adjustieren. Mit dieser Broschüre gehen wir einen weiteren Schritt in Richtung einer verbesserten IT-Sicherheit. Damit wollen wir am Digitalisierungs- und Wirtschaftsstandort Österreich die Datensicherheit verbessern und weitere Jobs kreieren. Ich wünsche Ihnen tolle Einblicke in die „Cyber Security Made in Austria“ sowie eine fesselnde Lektüre und praxisbezogene Erfahrungswerte.

KR Mag. Alfred Harl, MBA CMC
Obmann des Fachverbandes
UBIT der WKO

Bedrohung im Cyber-Raum kennt keine Grenzen

Cyber-Angriffe kennen keine Landesgrenzen. Informationssicherheit ist daher ein internationales Anliegen, das von einer länderübergreifenden Kooperation profitiert.

Als Cyber-Sicherheitsbehörde des Bundes gestaltet das Bundesamt für Sicherheit in der Informationstechnik, Bonn, die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft mit einem kooperativen Ansatz. Denn ein wirksames IT-Sicherheitsmanagement funktioniert nur mit einem stabilen Kontaktnetzwerk. So arbeitet das CERT-Bund des BSI national mit über dreißig CERTs im deutschen CERT-Verbund zusammen. Dies umfasst Unternehmens-, kommerzielle, akademische und Verwaltungs-CERTs auf Bundes- und Länderebene. Diese Kooperation bildet eine stabile Basis, um im Krisenfall gemeinsam, schnell und vertrauensvoll an Problemlösungen zu arbeiten.

Ebenso wichtig sind für das BSI die Kooperationen auf internationaler Ebene. In Europa zählt dazu neben der European Network and Information Security Agency (ENISA) die European Governmental CERT Group (EGC), ein informeller Zusammenschluss europäischer Regierungs-CERTs – in Österreich das vom Bundeskanzleramt in Kooperation mit dem CERT.at betriebene GovCERT Austria. Sie dient dem regelmäßigen Informationsaustausch über aktuelle Sicherheitsvorfälle und stärkt die Handlungsfähigkeit aller Partner. Die grenzüberschreitende Sichtweise sowie die verlässliche Partnerschaft ermöglichen auch im Krisenfall ein klares und differenziertes Bild der Lage.

„Informationssicherheit ist ein internationales Anliegen, das von einer länderübergreifenden Kooperation profitiert."

Veranstaltungen, wie das alle zwei Jahre

BSI CERT CYBER

Kooperation bildet eine stabile Basis, um im Krisenfall gemeinsam, schnell und vertrauensvoll an Problemlösungen zu arbeiten

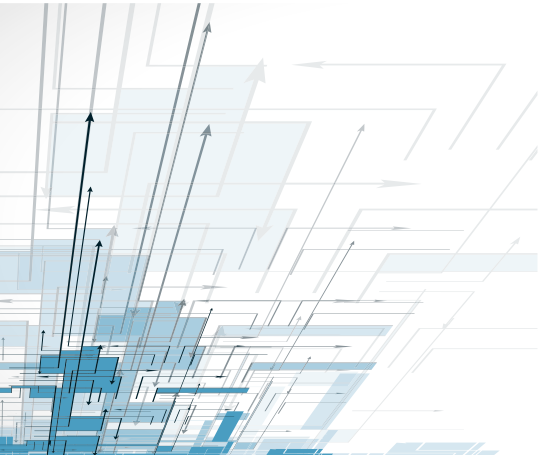
Denn ein wirksames IT-Sicherheitsmanagement funktioniert nur mit einem stabilen Kontaktnetzwerk

Als tragende Säule der Digitalisierung kommt vordergründig auch in Krisensituationen der Cyber-Sicherheit eine besondere Bedeutung zu

stattfindende Symposium „VIS!T – Verwaltung integriert sichere Informationstechnologie“, bilden eine wichtige Diskussions- und Austauschplattform für beispielhafte Lösungen und Herangehensweisen in der Cyber-Sicherheit. Das Symposium wird gemeinsam vom österreichischen Zentrum für sichere Informationstechnologie – Austria (A-SIT), dem Schweizer Informatiksteuerungsorgan des Bundes (ISB), der Agence nationale de la sécurité des systèmes d'information Luxembourg (ANSSI.lu) und dem BSI veranstaltet. 2020 fiel es leider wegen der Corona-Krise aus. Vor diesem Hintergrund wird deutlich, dass der Cyber-Sicherheit als tragende Säule der Digitalisierung vordergründig auch in Krisensituationen eine besondere Bedeutung zukommt.

Dank dieser IKT-Sicherheitsbroschüre ist ein toller Erfahrungsaustausch möglich sowie ein innovativer Wissensvorsprung im Themenkomplex der Cyber-Sicherheit erreichbar.

Ich wünsche Ihnen eine interessante und informative Lektüre.



Arne Schönbohm
Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Die Erfahrung der vergangenen Monate hat gezeigt, wie wichtig das Funktionieren der staatlichen Krisenmechanismen, die Aufrechterhaltung der kritischen Infrastruktur und die enge Zusammenarbeit zwischen Staat, Wirtschaft und Zivilgesellschaft für eine erfolgreiche Bewältigung der Covid 19-Krise waren und nach wie vor sind.

Die Bedrohungsszenarien für Österreich werden generell komplexer. Dies gilt umso mehr für die Herausforderungen, die mit Cybersicherheit und Digitalisierung verstärkt auf uns zukommen. Kriminelle Netzwerke nutzen vermeintliche oder tatsächliche Schwachstellen in Unternehmen aus, um BürgerInnen oder Institutionen anzugreifen. Umso wichtiger ist die intensive Beschäftigung mit Cyber Security als Grundprinzip der privaten und unternehmerischen Prävention sowie des Handelns im Anlassfall.

Die Studie „Cyber Security in Österreich" – die im heurigen Mai von KPMG und KSÖ veröffentlicht wurde – zeigt, dass 57 Prozent der Unternehmen in den letzten zwölf Monaten Opfer einer Cyberattacke wurden. 18 Prozent wissen gar nicht, dass sie angegriffen wurden. Besorgniserregend ist auch die Tatsache, dass nur 8 Prozent der befragten Unternehmen den Sicherheitsmaßnahmen ihrer Lieferanten und Dienstleister vertrauen. Es ist daher von größter Bedeutung, all diese Fragestellungen in das Zentrum der strategischen Ausrichtungen zu stellen: Der Bogen spannt sich hier von sicheren elektronischen Identitäten über die Sicherheit von Servern und jener bei Datenübertragungen bis hin zur Online-Sicherheit. All diese Aspekte werden in der vorliegenden IKT-Sicher-

„Sicherheit braucht die Zusammenarbeit und den Austausch aller Stakeholder – sei es aus Staat, Verwaltung, Wirtschaft, Forschung oder Zivilgesellschaft."

57% Unternehmen waren in den letzten zwölf Monaten Opfer einer Cyberattacke

18% Unternehmen wissen nicht, dass sie Opfer einer Cyberattacke waren

8% Unternehmen vertrauen ihren Lieferanten und Dienstleistern

heitsbroschüre umfassend aufgegriffen, wofür ich sehr dankbar bin.

Das KSÖ setzt eine Reihe von Maßnahmen, die diesen Entwicklungen gegensteuern. Dazu zählt ein „Sicherheitsforum für die Digitale Wirtschaft", das gemeinsam mit Unternehmen aus der kritischen Infrastruktur Strategien und Maßnahmen für eine sichere Digitalisierung entwickelt. Zudem hat das KSÖ gemeinsam mit dem Kreditschutzverband von 1870 eine Initiative gestartet, um ein Cyber Risk Rating in Österreich zu entwickeln. Damit sollen Unternehmen die Möglichkeit erhalten, den Grad der Vorbereitung und Professionalität ihrer Lieferanten und Dienstleister in Bereichen wie der Cybersicherheit oder dem Business Continuity Management zu prüfen.

Sie sehen, Sicherheit braucht die Zusammenarbeit und den Austausch aller Stakeholder – sei es aus Staat, Verwaltung, Wirtschaft, Forschung oder Zivilgesellschaft. Diese Broschüre soll Ihnen einen Wissensvorsprung und ein Rüstzeug bieten, ich wünsche Ihnen eine informative Lektüre.

© Eva Kelety

Mag. Erwin Hameseder
Präsident des Kuratorium
Sicheres Österreich (KSÖ)

INHALTSVERZEICHNIS

TOPIC 3 Cybercrime, Schadsoftware & Erste Hilfe

TOPIC 4 Forschung & Security-Ausbildung in Österreich

Integrierte Sicherheit für einen gestärkten Digitalisierungs- und Wirtschaftsstandort

Mag.ª Maria Ulmer

BMDW,
Sektionschefin

In der Verantwortung Ihrer Sektion liegen die Digitalisierung sowie E-Government für die Republik Österreich. Wie kann die Digitalisierung Arbeitsplätze schaffen?

E-Government trägt seit vielen Jahren maßgeblich zu einem modernen Wirtschaftsstandort bei. Heute schaffen wir digitale Amtswege nach dem Prinzip „Mobile Government" mit dem Once Only-Prinzip zur Vernetzung von Behördenwissen als Basis für No Stop Shops wie z.B. die antraglose Familienbeihilfe. Österreich gehört damit zu den Top 3 im E-Government der EU. Insgesamt ist die Digitalisierung ein Treiber für innovative Produkte, neue Geschäftsfelder oder Vertriebsformen wie E-Commerce und eine effizientere öffentliche Verwaltung. Diese Welle an Innovationen kann tausende Jobs schaffen, die ohne modernste Technologien der Digitalisierung gar nicht denkbar wären. Wir haben beispielsweise mit der elektronischen Unternehmensgründung ein attraktives Angebot für die Wirtschaft verfügbar.

Ist in unserem Cyber-Zeitalter die Digitalisierung zur Modernisierung der Verwaltung mehr Chance als Risiko? Welche Anstrengungen sind in Österreich erforderlich?

Digitalisierung ist zum einen Job-Motor und zum anderen Treiber für Veränderungen. Hier braucht es den Schulterschluss zwischen der gesamten Öffentlichen Verwaltung, Wirtschaft und der Gesellschaft wie z.B. bei der Schaffung der Plattform österreich.gv.at, der App „Digitales Amt", dem Unternehmensserviceportal USP oder dem Sicherheitsportal onlinesicherheit.gv.at. Ein Zukunftskapitel ist sicher auch der Aufbau einer vertrauenswürdigen Cloud-Infrastruktur in Europa. Angst muss niemand haben, denn die Chancen der Digitalisierung sollten dank integrierter Sicherheitsmechanismen auf organisatorischer und technischer Grundlage in Verbindung mit zielgerichteten Rechtsgrundlagen überwiegen.

Unsere vernetzte Welt wird immer digitaler. Wie beurteilen Sie die Sicher-

heit komplexer IT-Systeme als tragende Säule der digitalen Transformation?

Computer-Systeme werden immer aufwändiger und vielschichtiger. Auch die globale Vernetzung nimmt unentwegt zu. Durch die Komplexität verteilter Computer-Systeme bilden sich neue Angriffsflächen, die schwerer zu verteidigen sind. Demzufolge ist es heute notwendiger denn je, Sicherheit über den gesamten Lebenszyklus von IT-Systemen beginnend bei der Konzeption, über die Lieferkette bis zur Ablöse im Rahmen der digitalen Transformation von Prozessen einzubauen.

Ist Krisenfestigkeit und demzufolge Business Continuity insbesondere für kritische Systeme heutzutage neben der Sicherheit einer technischen Infrastruktur noch wegzudenken?

Bereits vor der Corona-Krise wurde der Digitale Aktionsplan Austria zur Schaffung einer „Digitalen Verantwortungsgesellschaft" mit den Themen Wachstum und Innovation ins Leben gerufen – jetzt ist das Thema Krisenfestigkeit dazu gekommen. Gleichzeitig hat die Republik aber gezeigt, dass sie bereits heute ihre Geschäfte im Krisenfall fortführen kann. Doch es gibt keine Krisenfestigkeit ohne IT-Sicherheit. Deshalb sind für besonders kritische IT-Systeme regelmäßige Risikoanalysen üblich und Business-Continuity-Maßnahmen sollten regelmäßig getestet und geprüft werden.

Nimmt die Bedeutung einer sicheren Identifizierung und Authentifizierung weiterhin rasant zu? Welche Entwicklungen und Trends erwarten Sie in den kommenden Jahren?

Mit der Bürgerkarte sowie der Handy-Signatur hatte Österreich bereits frühzeitig sehr innovative Produkte im Einsatz. Für Bürgerinnen und Bürger sind nun eine Vielzahl behördlicher Verfahren bequem 24 Stunden an sieben Tagen der Woche digital durchführbar. Der Nutzen elektronischer Identifizierungsmittel steigt in den kommenden Jahren durch eine tiefere Durchdringung unserer Gesellschaft und einer damit verbundenen, verbesserten Rechtssicherheit im digitalen Raum. Die Zukunft liegt im neuen elektronischen Identitätsnachweis ID Austria, der als wegweisende österreichische Lösung neue Funktionen mit sich bringt. Österreich hat eine Chance als digitaler Security-Leader mit vielen Jobs in diesem zukunftsorientierten Bereich.

Digitale Innovationen am Wirtschaftsstandort Österreich

Mag. Wolfgang Ebner

BMDW,
Präsident A-SIT

Schadsoftware breitet sich zunehmend aus, auch ist Resilienz eine grundlegende Forderung für kritische IT-Systeme. In welche Richtung entwickelt sich unser Digitalisierungs- und Wirtschaftsstandort?

Schadsoftware sorgt vermehrt für Ausfälle von Computersystemen und kompromittiert die Verfügbarkeit oft sensibler Daten. Angriffsziele sind zunehmend auch Unternehmen für Alltagsgüter. Die Sicherheit von Computersystemen ist ein wesentliches Fundament für einen starken Standort Österreich. Wir brauchen zielgerichtete Anstrengungen zur Entwicklung wegweisender Innovationen im Umfeld der Cyber Security. Das ermöglicht die notwendige Datensicherheit für komplexe IT-Systeme. Österreich soll sich zu einem digitalen Security-Leader entwickeln, um Sicherheit direkt in die Digitalisierung einzubauen und damit tausende Jobs zu schaffen.

Cloud-Systeme sind vordergründig wegen der Nutzung Mobiler Endgeräte seit Jahren auf dem Vormarsch. Welche Herausforderungen für die öffentliche Verwaltung und Unternehmen sehen Sie am Horizont?

Digitalisierung ohne zugrundeliegende Cyber Security ist riskant. Speziell komplexe Computersysteme sind lohnenswerte Angriffsziele. Demzufolge nehmen risikobasierte Ansätze für die Entwicklung von IT-Systemen eine besondere Bedeutung ein. Das umschließt auch den Betrieb dieser Systeme, wodurch etwa Business-Continuity und Resilienz vermehrt in den Brennpunkt rücken.
Darüber hinaus ist der Datenschutz eine wesentliche Herausforderung. Unser Ziel ist die Schaffung einer österreichischen Infrastruktur mit zwei Stoßrichtungen: Die Vernetzung österreichischer Cloud-Anbieter sowie eine Cloud-Lösung für User/innen, um Dokumente im Datensafe auf österreich.gv.at/ ablegen zu können. Für Unternehmen soll eine Lösung im Unternehmensserviceportal usp.gv.at/ geschaffen werden.

Das BMDW entwickelt als Partner Lösungen im Brennpunkt der Digitalisierung, um damit Bewusstsein für Cyber-Sicherheit zu schaffen. Auf welchen Plattformen sind verifizierte Informationen abrufbar?

Auf oesterreich.gv.at/ und der App „Digitales Amt“ können Amtswege elektronisch abgewickelt werden. Für die Wirtschaft sorgt das usp.gv.at/, FinanzOnline ist das wichtigste E-Government-Portal der Finanzverwaltung, dazu kommt das Transparenzportal. Das IKT-Sicherheitsportal onlinesicherheit.gv.at/ bietet Informationen zum sicheren Umgang mit Internet und das Rechtsinformationssystems ris.gv.at/ liefert entsprechende Einsichten. Die Initiative fit4internet.at/ und die kostenlose App „Cyber Security Quiz“ stärken digitale Kompetenzen.

Was ist notwendig, um die Chancen der Digitalisierung gemeinsam zu nützen, die Gefahren zurückzudrängen und somit in Österreich keine Zeit zu verlieren?

Gemeinsam mit Experten aus Wirtschaft, Verwaltung und Wissenschaft wird ein umfassendes strategisches Maßnahmenprogramm erarbeitet, damit Österreich die Chancen der Digitalisierung in den Bereichen Wirtschaft, Verwaltung, Bildung, Forschung und Innovation, Gesundheit und Pflege, Sicherheit und Infrastruktur bestmöglich und sicher nutzen kann. Dazu kommen der Ausbau und die Entwicklung neuer digitaler Services auf oesterreich.gv.at/, dem Digitalen Amt, aber auch dem usp.gv.at/. Gleichzeitig sollen für die Unternehmen Rahmenbedingungen rechtlicher und organisatorischer Natur so gestaltet werden, dass Innovationen noch einfacher und noch schneller möglich werden. Das schafft neue Arbeitsplätze.

In welcher Form und Geschwindigkeit entwickelt sich die Digitalisierung am Wirtschaftsstandort Österreich künftig? Gibt es Trends und damit verbundene Gefahren, die auf uns zukommen? Was erwarten Sie?

Österreich entwickelt sich dank Erfindergeist, unternehmerischer Wagnisse und des Einsatzes seiner Menschen in eine tolle Richtung. Doch müssen Veränderungen im Bereich der Digitalisierung beschleunigt werden. Aktuelle Trends wie Cloud-Systeme, Digitale Identitäten oder innovative Security-Lösungen zum Schutz mobiler Endgeräte befeuern diese Entwicklung. Im Bereich künstlicher Intelligenz gewinnt die digitale Ethik an Relevanz, Cyber Security ist im gesamten Lebenszyklus von IT-Systemen immer wichtiger.

Andreas Minnich
Abgeordneter zum Nationalrat

Cyber Security/Defense Organisationen & Staat

Wenn wir das Wort Digitalisierung verwenden, verbinden wir dies automatisch mit Cybersecurity. Was nützt heute das beste Produkt, welches unser Alltagsleben erleichtert, wenn es nicht die maximalen Sicherheitsanforderungen in seinem Lebenszyklus erfüllt?

Hackerangriffe in fast allen Bereichen und Branchen, gehören mittlerweile auch zum täglichen Leben. Aus diesem Grund benötigen wir in Österreich ein Fitnessprogramm für IT Security, um mit der fortschreitenden Digitalisierung weiterhin so gut mithalten zu können und damit wir weltweit – insbesondere im Bereich der Cloud-Systeme – nicht als Zuschauer auf der Tribüne sitzen müssen.

TOPIC 1

Cloud-Systeme

Security-Management

Cloud Computing

Herausforderung für die Verwaltung

Österreich hat frühzeitig einige Eckpfeiler für die Nutzung von Cloud-Technologien erarbeitet. Bislang war es aber vielen Verwaltungen kein brennendes Anliegen, auf Cloud-Technologien umzusteigen bzw. sich intensiv mit diesen auseinanderzusetzen. Die Lizenzpolitik von Microsoft und Co. hat diese Landschaft aber in der Zwischenzeit deutlich verändert und damit gab es auch wesentliche Gründe und Interessen, dieses Thema wieder auf die Tagesordnung zu bringen.

Mit der massiven Nutzung mobiler Geräte ist allen klar geworden, dass Cloud eine zentrale Technologie geworden ist. Alle mobilen Systeme leben in und von der Cloud und Europa ist hier auf die Zuseherränge verwiesen. Damit stellt sich vor allem für Verwaltungen, die neben den wirtschaftlichen Aspekten auch die Hoheits- und Souveränitätsfragen mit im Auge haben müssen, eine besondere Aufgabe. Diese Aufgabe ist umso schwieriger zu bearbeiten, als es keine EU-weit einheitliche Strategie und keine EU-weit anerkannten Prinzipien gibt, was wiederum mit dem unterschiedlichen Selbstverständnis und den unterschiedlichen gesetzlichen Randbedingungen der Verwaltungen zusammenhängt.

Neben der Wirtschaftlichkeit sind daher die nachfolgenden Themen zentral zu sehen:

› Verfügbarkeit auch in Zeiten der Krise. Diese Anforderung entsteht aus dem nicht delegierbaren Thema Souveränität, welches auch nicht outgesourced werden kann. Diese kann nicht mit wirtschaftlichen und damit versicherungstechnischen Mitteln kompensiert werden, sondern ist genuin durch den Staat wahrzunehmen. Als Folge daraus entsteht die Notwendigkeit – unabhängig von der Massennutzung eines Angebotes bzw. von Daten – Daten und Prozesse der Hoheitsverwaltung jedenfalls für Notsituationen jederzeit im Land verfügbar und im Backupbetrieb zu halten. Der Betrieb für normale und häufige Nutzung kann dabei bei Einsatz geeigneter Sicherungsverfahren durchaus im Wege der Cloud stattfinden.

„Mit der massiven Nutzung mobiler Geräte ist allen klar geworden, dass Cloud eine zentrale Technologie geworden ist."

› Für Informationen, die für das Staatsgeschehen innerhalb der Verwaltung zu verbleiben haben, sind deutlich strengere Maßstäbe anzusetzen. Es ist Stand des Wissens, dass vor allem durch

große Cloudanbieter zu den erst in den letzten beiden Jahren bekanntgewordenen Angriffen (Meltdown, Spectre und Co.) wirksame Gegenmaßnahmen nicht eingesetzt werden bzw. aus wirtschaftlichen Gründen nicht umgesetzt sind. Zu beobachten ist dies, weil in der verfügbaren Zeit die Voraussetzungen dafür nicht geschaffen werden können und die notwendigen Rechnerressourcen nicht am Markt verfügbar sind. Hier ist das Thema des massiv steigenden Energieverbrauches, den die Gegenmaßnahmen zwangsläufig mit sich bringen, noch gar nicht berücksichtigt. Dennoch sind derartige Risiken von Angreifern – vor allem staatlichen Angreifern und Spionagetätigen – durchaus realistisch. In diesem Bereich können neben der Verfügbarkeit nur Strategien angewendet werden, bei denen Daten ausschließlich in verschlüsselter Form in der Cloud und auf dem Kommunikationsweg dorthin und von dort vorliegen. Zudem muss gesichert sein, dass die Mechanismen der Verschlüsselung und insbesondere die Erzeugung von Schlüsseln hinreichend und abseits von fremdstaatlichen Interessen evaluiert sind und zur Gänze in der Kontrolle des Benutzers liegen. Dies schließt aber einige Formen der Cloud (etwa Software-as-a-Service) und vor allem viele Funktionalitäten wie etwa effiziente Suche nahezu aus.

- Während diese Prinzipien für isolierte Anwendungen einfach zu formulieren und im Einzelfall auch einfach umzusetzen sind, geht die allgemeine Entwicklung auch aufgrund der Lizenzpolitik von zentralen Softwareanbietern (Microsoft, Adobe,...) in eine diametral andere Richtung und es ist auch zu erwarten, dass dies die breite Nutzung, wie dies bei mobilen Geräten bereits geschehen ist, massiv beeinflussen wird.
- Ein weiterer Aspekt bei Services, die aus der Cloud bezogen werden, ist die unmittelbare Wirkung von Updates, wo der Anwender – auch wenn dieser Anwender ein Staat ist – nicht die Zeitpunkte und damit die Notwendigkeit, seine Services und seine Nutzung darauf abzustimmen, bestimmen kann. Dies könnte zwar durch strenge Rückwärtskompatibilität gelindert werden, doch zeigt die Erfahrung, dass diese in der Praxis

„Alle mobilen Systeme leben in und von der Cloud und Europa ist hier auf die Zuseherränge verwiesen."

durchaus anderen Zielen und Konzepten geopfert wird.

› Jedenfalls gilt es für Verwaltungen den regulatorischen Bedarf der eIDAS Richtlinie und den übrigen EU Vorgaben zu folgen. In diesem Punkt sind nahezu alle Cloudanbieter noch nicht vorbereitet, da etwa im US-Raum diese Aspekte noch nicht als Anforderung existieren. eID und elektronische Signatur müssen aber aus gesetzlicher Sicht umgesetzt sein und dies stellt einen weiteren Aspekt dar, warum Anwendungen, die Cloud nicht nur zum Datenspeichern verwenden, meist auf der Wartebank verbleiben.

Was die Nutzung von Cloud in der Verwaltung im EU-Raum deutlich vereinfachen könnte, wäre eine Europäische Cloud, die explizit die genannten Ziele mitumfasst. Das in Deutschland gestartete GAIA-X ist ein derartiger Ansatz auf Projektbasis, doch sind wir noch ein gutes Stück von der Praxis solcher Ansätze entfernt. Dies erklärt auch, warum nahezu alle EU Mitgliedsstaaten mit hoheitlichen Kernanwendungen (Budget, Militär, ...) sehr zurückhaltend bei der Nutzung von allgemeinen Cloud-Situationen sind. Dennoch ist es effizient und wichtig, die Strukturen der Anwendungen Cloud-fähig zu gestalten. Nicht nur, um für den Tag X gerüstet zu sein, sondern auch um Strategien wie Mobile First – und dafür gibt es einen massiven Bedarf – schon jetzt verfolgen zu können.

o. Univ. Prof. Dr. Reinhard Posch
Gesamtleiter A-SIT

„Für den sicheren Betrieb hochverfügbarer Applikationen und sensibler Daten ist eine enge Zusammenarbeit zwischen dem Bundesrechenzentrum und der A-SIT als staatlicher Verein für Sicherheit wichtig.

Durch diese Zusammenarbeit erhält das BRZ laufend aktuelle Forschungsergebnisse aus Bereichen wie Mobile Security, Access- und Identity Management oder Kryptographie. Mögliche zukünftige Schwachstellen können so frühzeitig erkannt und Vorkehrungen für die sichere Entwicklung kritischer Produkte und Services wie Video-Authentifizierung, elektronische IDs auf Smartphones, Zahlungssystemen uvm. getroffen werden."

Ing. Günther Lauer, Prokurist BRZ GmbH

A-SIT TIPP

Laut den Daten des Cybermonitors werden DDoS-Angriffe zwar immer intensiver, aber dauern im Durchschnitt immer weniger lang. Das BMF erarbeitete in Zusammenarbeit mit A-SIT Plus den Cloud Computing Kompass. Er beschreibt die strategische Planung zum Einsatz von Cloud Services. Beide sind abrufbar unter:

www.onlinesicherheit.gv.at

Weitere Informationen zur Entscheidungsfindung für den Einsatz von Cloud-Systemen sind im Österreichischen Informationssicherheitshandbuch zusammengefasst:

www.sicherheitshandbuch.gv.at

„Cloud-Technologien stellen vor dem Hintergrund der NIS-Richtlinie insbesondere kritische Infrastrukturen vor neue Herausforderungen. Sowohl die Standardisierung als auch die Bestätigung der Einhaltung von Sicherheitsanforderungen bilden Vertrauen. Der C5-Kriterienkatalog des BSI verschafft einen entscheidenden Wettbewerbsvorteil. Bestätigungen und Konformitätsbewertungen von A-SIT stärken das Vertrauen in die IT-Systeme“

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Entbürokratisierung durch Digitalisierung

MEHRWERT FÜR WIRTSCHAFT, WIRTSCHAFTSSTANDORT

Die Digitalisierung bestimmt als Thema und Motor Nr. 1 unsere Wirtschaft und unser alltägliches Leben. Es gibt unzählige Beispiele, die beweisen, wie innovativ Produkte Made in Austria im Digitalen Sektor sind. Von der Erfolgsstory der Handy-Signatur, Bürgerkarte, uvm. bis hin zur Möglichkeit, im digital gesicherten Raum Notariatsakte aus dem Ausland beim österreichischen Notar vor Ort durchführen zu können. Wir haben unzählige Beispiele für ausgezeichnete digitale Produkte, die unser tägliches Leben erleichtern und unseren Wirtschaftsstandort stärken.

> *„Forschung und Innovation im Sicherheitswesen sind für unseren Wirtschaftsstandort Österreich von wertstiftender Bedeutung. Der Bedarf der öffentlichen Verwaltung im Umfeld von Cloud-Technologien nimmt immer mehr zu. Dazu leistet A-SIT entscheidende Forschungsbeiträge."*

Aufgrund der aktuellen Pandemie, ausgelöst durch Covid-19, hat es in vielen Bereichen ein gewaltiges Umdenken und in gewisser Hinsicht auch Fortschritt gegeben. In diesem Zusammenhang muss man aber auch anmerken, dass es sowohl im staatlichen, wie auch im wirtschaftlichen und privaten Bereich noch einiges zu tun gibt, um die Digitalisierung als Chance und Erleichterung nutzen zu können. Komplexe bürokratische Strukturen zu digitalisieren löst nicht das eigentliche Problem, sondern spart höchsten einige Kilometer mit dem Auto, um etwa Dokumente künftig immer weniger physisch zu übermitteln.

Die aktuelle Situation hat uns unzählige Handlungsfelder aufgezeigt und auch Best-Practice-Modelle zum Vorschein gebracht. Es gilt, hier die notwendigen Schlüsse zu ziehen, zu lernen und vor allem die erkannten Probleme und Fehler zu bearbeiten und nicht im Zuge der werdenden Normalisierung zu vergessen. Dieser Schritt ist notwendig, um gestärkt aus der Krise zu gehen. Die Digitalisierung bringt für alle Akteure, egal in welchem Bereich, immense Chancen sowie natürlich auch viele Risiken. Man sollte hier, egal von welcher Seite, auf keinen Fall Angst haben, denn sonst haben wir im Wettlauf der Digitalisierung keine Chance. Es gilt, die Brücke zwischen unkomplizierten und logischen Abläufen und der höchst möglichen Sicherheit zu bauen.

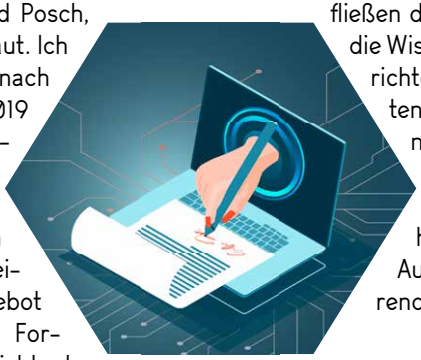
Andreas Minnich

Abgeordneter zum Nationalrat

Die Rolle von A-SIT und E-Government am IAIK

Die TU Graz ist als Gründungsmitglied seit 1999 Teil von A-SIT und bildet dessen wissenschaftliche Basis. Seit 2005 betreiben wir auch das E-Government Innovationszentrum EGIZ, ursprünglich zusammen mit dem Bundeskanzleramt, nun mit dem Bundesministerium für Digitalisierung und Wirtschaftsstandort BMDW. Der Themenbereich rund um E-Government, elektronische Signatur und elektronische Identität wurde von meinem Vorgänger als Institutsvorstand des IAIK, Prof. Reinhard Posch, mit viel Einsatz aufgebaut. Ich durfte diese Erfolge nach seiner Emeritierung 2019 übernehmen und weiterführen.

„Aktuelle Schwerpunkte sind etwa die Unterstützung der Mobile First Strategie oder elektronische Vertretung im grenzüberschreitenden Verfahren."



Wir sehen mit dem mittlerweile schon breiten produktiven Angebot an E-Government den Forschungsbedarf aber nicht als beendet an, im Gegenteil: Es werden mit dem Druck zu weiterer Digitalisierung die Herausforderungen weiter steigen. Mobile Endgeräte, Cloud Computing oder Once-Only sind nur einige Schlagworte aktueller Herausforderungen, die der öffentliche Sektor samt der mit neuen Technologien einhergehenden und typisch steigenden Dynamik bewältigen muss. Hier kann wissenschaftliche Forschung ansetzen, um in die technologische Innovation von Beginn an Datenschutz und Informationssicherheit einzubringen.

Die Forschung dazu haben wir im Bereich „Secure Applications" zusammengefasst, in dem immerhin etwa 30 Forscherinnen und Forscher tätig sind. Aktuelle Schwerpunkte, an denen der Bereich forscht, sind etwa die Unterstützung der Mobile First Strategie oder elektronische Vertretung im grenzüberschreitenden Verfahren. Im Sinn forschungsgestützter Lehre fließen die Erkenntnisse auch in die Wissensvermittlung ein. So richten sich unsere Aktivitäten über A-SIT und EGIZ nicht nur an die Bedarfsträger des öffentlichen Sektors, sondern wir haben immer auch die Ausbildung der Studierenden im Blick.

Univ.-Prof. Dr. Stefan Mangard

Institutsvorstand IAIK,
TU Graz

Risikoanalysen als Grundlage

sicherer IT-Infrastrukturen in Unternehmen

In unserer zunehmend digitalisierten Welt hängt der Erfolg von Unternehmen in steigendem Maße von der Sicherheit und Verfügbarkeit ihrer IT-Infrastrukturen ab. Mit der stetig steigenden Komplexität dieser IT-Infrastrukturen nimmt jedoch auch die Bedrohungslandschaft immer schwerer zu überblickende Ausmaße an. Unternehmen stehen damit vor der Herausforderung, theoretisch einen immer größeren Ressourcenaufwand treiben zu müssen, um sich und ihre IT-Infrastruktur adäquat gegen alle möglichen Bedrohungen zu schützen. In der Praxis tun sich dabei rasch Grenzen auf, da tatsächlich verfügbare finanzielle und personelle Ressourcen beschränkt sind. Für Entscheidungsträger stellt sich somit die Frage, wo und wie die limitierten Ressourcen am effektivsten eingesetzt werden sollen.

In der Praxis ist diese Frage meist nicht einfach zu beantworten. Zu komplex sind die Abhängigkeiten von Erfolgsfaktoren des Unternehmens zu den diversen Komponenten der IT-Infrastruktur. Zudem sind Abhängigkeiten aufgrund der Gesamtkomplexität in vielen Fällen auch gar nicht bewusst. Je größer und komplexer das Unternehmen und seine IT-Infrastruktur, desto schwieriger ist der zielgerichtete und möglichst effektive Einsatz verfügbarer Ressourcen zur Erhöhung der IT-Sicherheit im Unternehmen.

Systematische Risikoanalysen können hier Abhilfe schaffen. Ziel ist dabei die Erstellung eines abstrakten Risikomodells des Unternehmens, über das Abhängigkeiten zwischen kritischen Geschäftsprozessen auf der einen und relevanten Komponenten der IT-Infrastruktur auf der anderen Seite modelliert werden. Das Risikomodell bildet einerseits die Kritikalität von Geschäftsprozessen über deren Schutzbedarfe ab und stellt andererseits die Abhängigkeit der diversen Geschäftsprozesse von der Sicherheit verwendeter IT-Komponenten dar. So wird über das Risikomodell unmittelbar ersichtlich, welche Auswirkung die theoretische Kompromittierung einer IT-Komponente auf die diversen Geschäftsprozesse und damit auf den Erfolg des Unternehmens hätte. Über das Risikomodell können also jene Komponenten der IT-Infrastruktur identifiziert werden, die kritisch für den Erfolg des Unternehmens sind. Über die systematische Betrachtung relevanter Bedrohungen für die einzelnen modellierten IT-Komponenten können zudem notwendige Maßnahmen zu deren Schutz systematisch abgeleitet werden. Über die aus dem Modell ersichtliche Kritikalität einer Komponente kann die Umsetzung von Maßnahmen zu ihrem Schutz priorisiert werden.

„Über das Risikomodell können also jene Komponenten der IT-Infrastruktur identifiziert werden, die kritisch für den Erfolg des Unternehmens sind."

Der Nutzen eines über eine systematische Risikoanalyse erstellten Risikomodells hängt stark von seinem Detaillierungsgrad ab. Die Erstellung eines möglichst detaillierten Risikomodells kann selbst rasch zu einem zeitaufwändigen Unterfangen werden, dessen Komplexität ab einem gewissen Punkt nur mehr durch die Verwendung einschlägiger Tools beherrschbar bleibt. Zu beachten ist in diesem Zusammenhang auch, dass die Erstellung eines Risikomodells keine einmalige Anstrengung sein darf, sondern als kontinuierlicher Prozess begriffen werden muss. Nur so ist gewährleistet, dass laufende Transformationen und Weiterentwicklungen des Unternehmens und seiner IT-Infrastruktur im erstellten Risikomodell berücksichtigt werden und das Modell so stets ein akkurates Abbild des realen Unternehmens bleibt.

Die Durchführung systematischer Risikoanalysen über die Erstellung eines Risikomodells ist ein herausforderndes Unterfangen, in dem stets ein passendes Gleichgewicht zwischen einem möglichst hohem Detaillierungsgrad auf der einen und einer bestmöglichen

Beherrschung der Komplexität auf der anderen Seite gefunden werden muss. Für einen effektiven und zielgerichteten Einsatz verfügbarer finanzieller und personeller Ressourcen zur Verbesserung der IT-Sicherheit eines Unternehmens und seiner IT-Infrastruktur ist die Durchführung systematischer Risikoanalysen jedoch alternativlos.

Dr. Thomas Zefferer

Senior IT Security Expert
A-SIT Plus GmbH

„Security-Lösungen Made in Austria bringen Innovationen auf den Boden."

Andreas Minnich

Verbesserung der Cyber-Resilienz für Behörden und Unternehmen

DI Mag. Andreas Tomek

Partner, Advisory
KPMG Austria

DI (FH) Robert Lamprecht MSc

Director, Advisory
KPMG Austria

18% der Unternehmen wissen laut Ihrer Cyber-Security-Studie nicht, ob sie angegriffen wurden. Wie wird Cyber-Security ein Wettbewerbsvorteil für Österreich?

RL: Cyber-Security ist zum Schutz und Überleben von Unternehmen ein kritischer Erfolgsfaktor. Leider kümmert sich häufig niemand darum und auch das Bewusstsein dazu fehlt sehr oft. Demzufolge besteht Handlungsbedarf vordergründig in organisatorischem Hinblick und im Gleichklang mit der Umsetzung einer notwendigen technischen Ausstattung. Das ist natürlich mit spezialisierter, externer Hilfe erreichbar. Diese Art von Unterstützung bieten und realisieren wir bei KPMG.

AT: Genau, große Unternehmen sind zwar zur Behandlung von Security-Herausforderungen vermehrt gut ausgerüstet, aber es gibt auch Lücken. Interesse besteht zunehmend im KMU-Bereich. Generell sind nachhaltige Veränderungen schwer umzusetzen und es hapert beim Mindset. Oft fehlen die Skills sowie die notwendigen Tools und die vorhandenen Regelwerke sind unzureichend. Damit wir das beheben können, braucht es gezielte Investitionen und gut ausgebildete Fachkräfte, um den Zugang zu Technologien zu vereinfachen und um Vertrauen aufzubauen.

Wie sehr vertrauen die Unternehmen ihren eigenen Schutzmaßnahmen und führt das zu einem falschen Sicherheitsgefühl?

RL: Natürlich braucht es eine gewisse Vertrauensbasis – ohne diese kommen wir nicht weit und ja, Unternehmen fühlen sich oftmals schon sehr sicher. Das ist natürlich ein Alarmsignal, denn dieses Sicherheitsgefühl ist oft trügerisch. Allerdings führt etwa die mediale Berichterstattung vielfach zu Unsicherheit. Denn es gilt: Ist ein Cyber-Angriff einmal da, dann geht es schnell und der Schaden ist hoch. Daher braucht es nachgeschärfte – etwa gesamtstaatliche – Cyber-Security-Lagebilder, die Entscheidungsträgerinnen bzw. Entscheidungsträgern mit den richtigen Informationen versorgen. Aber Achtung, Eigenverantwortung ist unerlässlich und setzt den Mut zur offenen Kommunikation und zum aktiven Informationsaustausch voraus, um den Schutz gegen Cyber-Risiken zu forcieren. Daher ist der Austausch mit Behörden und Security-Communities ausgesprochen wertvoll und wichtig.

Welche Veränderungen hat Österreich wegen intensiver Digitalisierung in den letzten Jahren durchgemacht? Was sind die größten Herausforderungen und Trends?

AT: Gerade Krisen wie Pandemien beschleunigen die Digitalisierung. Dadurch gab es eine Verdichtung im Bereich der Mobilität und der Vernetzung. Zu erwarten sind zum einen vermehrt neuartige, digitale Produkte und Services. Zum zweiten sehen wir eine beschleunigte Digitalisierung bei klassischen Geschäftsmodellen. Aber wir haben gelernt: Vertrauenswürdige Produkte erfordern geeignete Schutzmaßnahmen im gesamten Lebenszyklus von IT-Systemen. Da ist Schnelligkeit leider für die Sicherheit manchmal hinderlich.

RL: Es stimmt, dass Vertrauen in digitale Services für Behörden bzw. in digitale Geschäftsmodelle und Produkte für Unternehmen von maßgeblicher Bedeutung ist. Für eine langfristige Widerstandsfähigkeit von Produkten und Services benötigen wir Vertrauen zu den Zulieferern und geeignete Schutzmechanismen.

Wodurch können Behörden und Unternehmen langfristig widerstandsfähiger gegen schwer erkennbare Cyberattacken werden sowie rasch auf Krisen reagieren?

RL: Da die Uhr tickt, wenn der Alarm losgeht, muss sich vordergründig das Mindset ändern und „consider your network breached“ die oberste Devise sein. Für Behörden ist das schwerer als für Unternehmen. Andererseits ist Prävention sehr wichtig, aber leider ist diese allein nicht ausreichend. Wir müssen schneller reagieren und in Zusammenhängen denkend handeln. Egal ob mit internem Personal oder durch strukturierte externe Unterstützung. Dabei helfen wir bei KPMG sehr gerne.

AT: Wichtig ist, wenn es darauf ankommt, die richtigen Entscheidungen zu treffen. Daher geht es vermehrt um Menschen und Prozesse – weniger um Technik. Gut ausgebildetes Personal ist aber schwer zu finden. Zu wenige Menschen haben Erfahrungen mit der strukturierten Lösung komplexer Cyber-Angriffe, da in Österreich die richtig großen Erfahrungswerte fehlen.

RL: Richtig, gerade die Durchhaltefähigkeit wird unterschätzt. Diese ist für resiliente Organisationen eine Grundvoraussetzung. Cyber-Angriffe sind meistens nicht nach einem Tag vorbei, aber Menschen sind nach 24h müde. Hier braucht es Lösungen.

Komplexe Angriffe sind schwer zu erkennen. Wie finden Behörden und Unternehmen den richtigen Weg, um den Durchblick für Cybersicherheit zu erhalten und damit die Aufgaben aufrecht zu halten?

RL: Die Vergangenheit zeigt, dass neben Technologiekonzernen auch Konsumgüterunternehmen oder Firmen im Logistik-Bereich lohnenswerte Angriffsziele sind. Als Menschen und als Gesellschaft müssen wir lernen, dass das unscheinbare Thema Cyber-Security heute lebensnotwendig ist. Die Angreiferinnen bzw. Angreifer schlafen nicht und die Attacken führen zu massiven Schäden in unserer Gesellschaft. Manche davon werden für lange Zeit übersehen. Wir sind aber nicht hilflos. Wenn wir mit einem geordneten Fokus einen kühlen Kopf bewahren, dann können wir mit der richtigen Einstellung und der Anwendung geeigneter Tools im Rahmen eines zielgerichteten Regelwerks die Schäden minimieren. Dafür braucht es die Analyse der jeweiligen Situation. Das bindet zum einen Ressourcen und setzt zum anderen die passenden Skills voraus. Diese Ressourcen sind notwendig.

Welche Investitionen in Cybersicherheit sind besonders schlagkräftig?

AT: Einerseits muss man aufpassen, sich selbst nicht zu überschätzen sowie Andere nicht zu unterschätzen und die Erwartungen müssen klar sein. Andererseits gilt mehr denn je „Trust but verify“. Dafür sind Prüf-Mechanismen und Security-Managementsysteme notwendig, um die oft kostengünstigere Auslagerung der Daten in Cloud-Systeme zu evaluieren. Aber ohne technische Verfahren wie etwa Verschlüsselung ist der Schutz der Daten nicht erreichbar. Und das hat uns COVID-19 eindrucksvoll gezeigt.

RL: Richtig, wir haben gesehen, dass die beschleunigte Digitalisierung durch COVID-19 quasi über Nacht geliefert wurde. Nur, eine Verlagerung in die Cloud löst nicht alle Probleme und es eröffnen sich neue Herausforderungen. Das sogenannte „Third-Party-Risk-Management“ ist gerade bei der Verwendung von Cloud-Systemen besonders relevant, da nur 8% der Unternehmen in die Sicherheitsmaßnahmen der Lieferanten vertrauen. Geprüft wird aber leider zu wenig. Darauf aufbauend sollten wir Geschäftsmodelle verändern und neue Chancen ergreifen, damit die Anstrengungen zu mehr Cyber-Security intensiviert werden.

Sicherheit schafft Klarheit. Klarheit sichert Vertrauen.

Der öffentliche Sektor ist uns ein persönliches Anliegen:
Ob Gesundheit, Verkehr oder Bildung – der technologische Wandel betrifft alle Bereiche. Unsere Cyber Security-Experten schaffen Klarheit und stehen Ihnen als Mitstreiter zur Seite.
Wir begleiten Sie auf Ihrem Weg in die digitale Zukunft.

Erfahren Sie mehr: kpmg.at

KPMG

Neue Verschlüsselungstechnologien

für smarte Cloudlösungen von morgen

Die voranschreitende Digitalisierung und globale Vernetzung in allen Lebens- und Wirtschaftsbereichen hat durch die umfassende Verwendung von virtuellen IT-Diensten – Cloud Services – eine neue Dimension erreicht. Cloud Angebote sind die Grundlage für geringere Investitionskosten in IT-Infrastrukturen, kürzere Time-to-Market Intervalle, geringeres IT-Risiko durch Fokussierung auf das wirklich notwendige, und schließlich höhere Innovationskraft, weil dadurch neue IT-Dienste rascher verwendet und verändert werden können. Somit werden unsere Daten immer umfassender in der „Cloud" gespeichert und verarbeitet.

Damit ändert sich nun aber auch ein wesentliches Paradigma in unseren Informations- und Kommunikationstechnologien. Die letzten 30 Jahre haben wir uns vorranging darauf konzentriert, unsere Daten sicher und verschlüsselt zu übertragen und zu speichern. Durch die laufend neu hinzukommenden virtualisierten IT Systeme erhalten wir jedoch nun eine veränderte Bedrohungssituation. Denn durch den mittlerweile allumfassenden Einsatz von Cloud-Diensten gibt es heute keine echte Ende-zu-Ende Sicherheit der Daten mehr. Wir haben keine volle Gewissheit mehr, was in der Cloud mit unseren Daten passiert. Darüber hinaus gilt es auch zu beachten, dass es nicht nur um die Sicherheit der Daten selber geht, sondern dass auch die relevanten Metadaten, die oft sehr viel über den Benutzer aussagen, als kritische Information gesehen werden muss, die es besonders zu schützen gilt. Zurzeit bleibt uns aber nichts anderes übrig, als dem jeweiligen Cloud-Anbieter zu vertrauen, dass er die ihm anvertrauten Daten vereinbarungsgemäß behandelt.

Wir leben mittlerweile in einer Gesellschaft, die sich schon an die vielen Cloudservices gewöhnt hat, auch wenn unsere Daten nicht unbedingt als sehr geschützt zu betrachten sind. Viele Serviceanbieter fangen die Kunden mit angeblichen Gratis-Dienstleistungen. Dabei wird häufig nicht wahrgenommen, dass man mit der Zurverfügungstellung seiner Daten oft mit dem Preis der Privatsphäre bezahlt. Bei näherer Betrachtung gibt es allerdings triftige Gründe, warum wir alle mehr Augenmerk auf den Schutz unserer Daten legen sollten – vor allem wenn man berücksichtigt, dass die umfassende Digitalisierung und globale Vernetzung eine neue Skalierbarkeit der Datenanalyse mit sich bringt: für den Datenanalysten ein Segen, für unsere Privatsphäre potentiell ein Fluch.

„Bei näherer Betrachtung gibt es allerdings triftige Gründe, warum wir alle mehr Augenmerk auf den Schutz unserer Daten legen sollten."

Warum sollen wir nun aber unsere Daten schützen?

- Für viele Anbieter ist der Zugriff auf unsere Daten und/oder Metadaten die Grundlage ihrer Geschäftsmodelle;
- für Unternehmen ist wohl der Schutz der Unternehmensdaten eine der wichtigsten Geschäftsgrundlagen; und
- für Privatpersonen ist die Vermeidung der missbräuchlichen Verwendung von persönlichen Daten die Grundlage für eine funktionierende Gesellschaft.

Dadurch ergibt sich ein heute vielfach verfolgtes Geschäftsmodell für lokale Service Provider, in dem Cybersicherheit und Schutz der Privatsphäre vor allem über den z.B. europäischen Standort der Servicebetreiber argumentiert und darüber eine sichere Datenverarbeitung als USP verkauft wird.[1], [2]

Allerdings werden in Zukunft leistungsfähigere Verschlüsselungstechnologien notwendig sein, um IT-Innovationen zu ermöglichen, aber auch gleichzeitig höchsten Schutz unserer Daten sicher zu stellen. Auch müssen wir uns darauf einstellen, dass mögliche Quantencomputer unsere existierende asymmetrische Verschlüsselungstechnik bedrohen und unsere Daten potentiell entschlüsseln werden können. Aktuelle Forschungsprogramme arbeiten nun

intensiv an smarten Verschlüsselungstechnologien mit einem inhärenten „Privacy by Design" zum Schutz unserer Daten in Cloud Systemen, damit neue Lösungen für einen selektiven und flexiblen Zugang zu Daten und eine sichere Informationsteilung unterstützt sowie eine digitale Souveränität nachhaltig sichergestellt werden können.[3]

Folgende Bereiche brauchen neue kryptographische Verfahren:

- Sicheres Speichern und Teilen von Daten in der Cloud: Für ein dynamisches und selektives Teilen von Daten in der Cloud unter mehreren Benutzern werden neue sogenannte „attribute based encryption" (ABE) Techniken entwickelt. ABE Systeme erlauben einen selektiven Zugriff auf Daten, wie z.B. den selektiven Zugriff auf verschiedene Inhalte von Dokumenten durch unterschiedliche Benutzer[4]. Dadurch ist keine komplizierte IT-Landschaft für das Regeln von Datenzugriffen oder das Vertrauen in Service-Provider mehr notwendig.

(1) Austrian Cloud: Quality seal for cloud providers keeping all data in Austria, https://www.wko.at/branchen/w/informationconsulting/austrian-cloud.html
(2) European Cloud Initiative: Strengthen Europe's position in data-driven innovation, improve competitiveness, and help create a Digital Single Market, https://ec.europa.eu/digital-single-market/en/european-cloud-initiative
(3) Neue Bedrohungen für unsere alten Daten, 11.5.2020, https://scilog.fwf.ac.at/natur-technik/11564/neue-bedrohungen-fuer-unsere-alten-daten
(4) EU-H2020 Projekt PRISMACLOUD, https://www.prismacloud.eu

Die Zugriffsregeln sind in der Verschlüsselungstechnik direkt eingebettet. Mit smarten Verschlüsselungstechnologien können auch smarte Cloud-basierte Datenspeicherlösungen durch Informationsteilung auf mehrere Serverstandorte erreicht werden. Die Daten werden dabei geschickt auf mehrere Cloud-Standorte aufgeteilt, wobei kein einzelner Betreiber der Cloud-Services die Daten lesen oder bearbeiten kann. Anderen Personen kann dadurch auch dynamisch und flexibel ein selektiver Datenzugriff gewährleistet werden und man muss nicht in einem IT System starre Zugriffsregeln festlegen.[5], [6], [7]

- Schutz der Datenintegrität: Eine Authentizität der Daten wird für zukünftige Datenmärkte ein entscheidender Faktor sein, um eine Aggregation von verschiedenen Datenquellen zu unterstützen. Ein Ausblenden (Schwärzen) von einzelnen Datenteilen ermöglicht ein einfaches selektives Teilen von Daten in der Cloud.[8]
- Sicheres Rechnen in der Cloud: Die Möglichkeit von Berechnungen auf verschlüsselten Daten ermöglicht eine Cloud-Nutzung und Zusammenarbeit ohne Aufgabe der Datenhoheit. Die Mächtigkeit neuer kryptographischer Verfahren demonstriert die Auktionsplattform für Produktionskapazitäten der Firma Catch GmbH als ein Musterbeispiel für ein neues Industrie 4.0 Geschäftsmodell. Betreiber von Produktionsmaschinen können ihre freien Produktionskapazitäten auf einer Auktionsplattform anbieten bzw. nach Produktionskapazitäten bei anderen Produzenten suchen. Dabei erfolgt keine zentrale Datenhaltung, sondern der Datenabgleich erfolgt in einer dezentralen IT-Architektur auf vollständig verschlüs-

(5) FFG gefördertes Projekt ARCHISTAR, http://archistar.at und Lösungsangebot der Firma fragmentiXTM, https://www.fragmentix.com/
(6) ETSI releases cryptographic standards for secure access control, Sophia Antipolis, 21 August 2018, https://www.etsi.org/newsroom/press-releases/1328-2018-08-press-etsi-releases-cryptographic-standards-for-secure-access-control
(7) ETSI TS 103 458, Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements, V1.1.1, Juni 2018, https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf
(8) ISO/IEC DIS 23264-1, Information security — Redaction of authentic data — Part 1: General, https://www.iso.org/standard/78341.html

selten Daten.[9] Die Produktionsdaten können von den Teilnehmern allerdings nicht gesehen oder analysiert werden. In gleicher Weise ermöglicht die Anwendung spezieller Machine Learning Verfahren („privacy preserving machine learning") neue Geschäftsmodelle und Ansätze für eine intelligente Datenverarbeitung, ohne dass die einzelnen Daten für die Benutzer lesbar sind.[10]

› Online Privacy: Wie im richtigen Leben will man auch online verschiedene Identitäten haben. Eine anonyme Authentifizierung ermöglicht auch eine digitale Privatsphäre und verhindert eine vollständige Nachverfolgungsmöglichkeit der Benutzeraktivitäten für Cloudbetreiber. Ein modernes Identitätsmanagement Service (IDMaaS) zur Authentifizierung bei verschiedenen Cloud Service Anbietern wird in der EU Forschungsinitiative Credential verfolgt.[11] Anonyme Anmeldedaten (credentials) erlauben eine Benutzer-zentrierte kryptographisch geschützte Authentifizierung bei mehreren Service Anbietern, ohne dass ein zentraler Cloudanbieter alle Anmeldevorgänge mitbeobachten und analysieren kann, wie es z.B. bei vielen Services heute passiert, wenn man sich bei mehreren Services mit einem Google oder Facebook Account anmeldet.

Eine digitale Datensouveränität ist eine unserer grundlegenden Herausforderungen im Cloud-Zeitalter. Wir brauchen dafür smarte und intelligente Lösungen. Dies erreichen wir durch Forschung und Entwicklung in Kombination mit der erforderlichen engen Kooperation zwischen Service Betreibern und Anwendern, um nachhaltige und effektive Lösungen für unsere digitale Zukunft zu bauen.

(9) FFG gefördertes Projekt FlexProd, https://flexprod.at/
(10) EU-H2020 Projekt KRAKEN, https://krakenh2020.eu/
(11) EU-H2020 Projekt CREDENTIAL, https://www.credential.eu

DI Helmut Leopold, PhD

Head of Center
for Digital Safety & Security,
AIT Austrian Institute of Technology

Vertrauen als Grundlage

für die Beschaffung sicherer Hardware und Software

Die Vertrauenswürdigkeit des Anbieters und Herstellers und die IT-Sicherheit des Produkts sollen die Grundlage für die Beschaffung sicherer HW und SW darstellen. Dabei stellen die Nutzung von anerkannten Sicherheitsstandards, Richtlinien, anerkannte Zertifizierungen wie Common Criteria, Gütesiegel und Best Practice Methoden eine gute Basis dar, um beim Kunden Vertrauen zu schaffen. Ebenso sind IT-sicherheitsrelevante Referenzen und Erfahrungsberichte von anderen Kunden hilfreich.

Alle Nutzer von IKT sind zu einem gewissen Grad von ihren Herstellern abhängig. Durch die Globalisierung der Produkt-Lieferkette interagieren immer mehr Akteure, um ein Produkt zu produzieren. Zur Vertrauenssicherung hat jeder Akteur der Produktlieferkette die Verantwortung, die erforderliche IT-Sicherheit und Widerstandsfähigkeit des Produkts vor Angriffen von außen zu gewährleisten. Entsprechend des ISO/IEC 27002 Standards sind die Sicherheitsanforderungen für die Anbieter auch den vorgelagerten Unternehmen (Hersteller, Sublieferanten) aufzuerlegen.

„Alle Nutzer von IKT sind zu einem gewissen Grad von ihren Herstellern abhängig."

Ebenso helfen sogenannte „Bug Bounty Programme", wo Personen aufgefordert werden, IT-sicherheitsrelevante Schwachstellen bei einem Fund an den Hersteller und dieser wiederum zu seinen Kunden zu melden. Als Belohnung erhält der Finder bzw. die Finderin je nach Kritikalität der Schwachstelle eine entsprechend hohe Aufwandsentschädigung.

Des Weiteren ist für das Vertrauen auch eine Recherche bezüglich IT-Sicherheitslücken und IT-Sicherheitsvorfällen wichtig. Dabei spielen die verschiedenen CERTs eine große Rolle. Auch die Eigentümer und die Herkunft des Herstellers und Anbieters können einen großen Einfluss auf das Vertrauen haben. Dabei spielen Medienberichte über bewusst eingebaute Schwachstellen eine Rolle.

Zur Vertrauensbildung kann auch gehören, dass der Lieferant für das zu beschaffende Produkt alle zutreffenden IT-Sicherheitsanforderungen in der Beschaffungsplattform it-sicher.kaufen/ ankreuzt und die daraus automatisch generierten Texte in den Kaufvertrag übernimmt.

Plattform IT - sicher.kaufen

(https://www.it-sicher.kaufen/)

Funktion und Preis spielen bei der Beschaffung von Software meist die zentrale Rolle. Kaum jemand schaut dabei auf die IT-Sicherheit. Etwas Unsicheres zu kaufen kann später aber sehr teuer werden. Die Beschaffungsplattform it-sicher.kaufen/ als Ergebnis eines KIRAS-Forschungsprojektes der FFG liefert kostenlos, herstellerunabhängig, werbefrei und passend zu den individuellen Ansprüchen die wichtigsten Informationen für eine Beschaffung von IT-sicherer Hardware (HW) und Software (SW). Sie enthält vor allem IT-Sicherheitsanforderungskataloge. Dabei wird unterschieden zwischen Standard-SW, Individual-SW (in Auftrag gegebene SW) und HW mit integrierter SW (Firmware, embedded SW). Für jede dieser Kategorien gibt es für die IT-Sicherheitsanforderungen eine Überblicksversion (ca. 3 Seiten) sowie eine Langversion.

Auf der Plattform können Beschaffer durch Ankreuzen auswählen, welche Parameter für ihre Produkte wichtig sind. Beispielsweise sind dies bei Standardsoftware Aspekte der Benutzerauthentifizierung und Zugriffskontrolle, Fehlerbehandlung und Protokollierung, Konfiguration, Datenschutz, Spionage und Sabotage, Vertraulichkeit und Dokumentation, bei HW mit embedded SW sind dies Anforderungen an Zulieferer und Bauteile, Updates und Informationspflicht, Entwicklung und Dokumentation, Produkthärtung und Malware- und Manipulationsfreiheit bei der Auslieferung.

„Unsichere Software zu kaufen kann später sehr teuer werden."

Nach der Auswahl durch den Beschaffer werden von der Plattform automatisch Checklisten bzw. Templates als Word- oder pdf-Datei erstellt, die beim Kontakt mit Anbietern als Fragebogen oder als Textbausteine für öffentliche Ausschreibungen oder Lastenhefte verwendet werden können. Zu jedem Punkt gibt es auch einen umfangreichen erklärenden Text mit weiteren Informationen.

Des Weiteren enthält die Plattform Informationen, was bei der Beschaffung von quelloffener SW (Open Source SW bzw. freie SW) zu beachten ist.

Als wichtige Ergänzung zur Plattform dient das erschienene Buch „Beschaffung unter Berücksichtigung der IT-Sicherheit" im Springer Verlag.

Univ.-Doz. DI Dr. Ernst Piller

FH-Professor
Institut für IT-Sicherheitsforschung,
FH St. Pölten

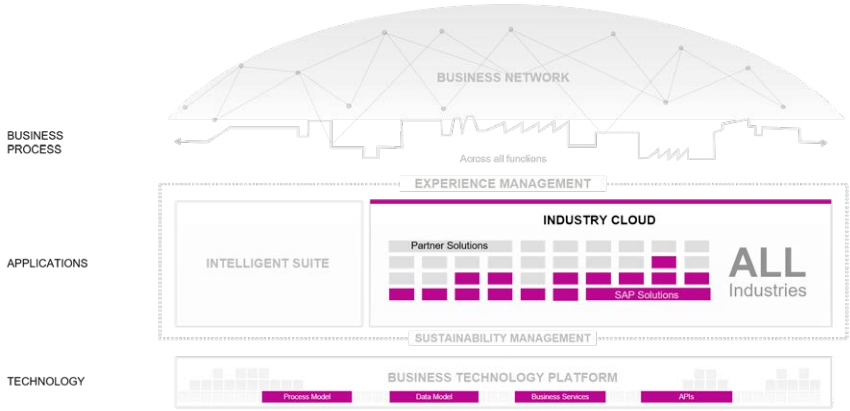
Sichere Cloudsysteme für kritische Anwendungen im Behördenumfeld

Heinrich Pfriemer

Global Head Industry Business Unit Defense and Security
SAP

Welche Vorteile bieten Cloudsysteme gegenüber eigener On-Premise-Lösungen?

Die Vorteile von Cloudsystemen liegen auf der Hand, es geht den Kunden um Wahlmöglichkeit, Skalierbarkeit und rasche Implementierung von Prozessen und Innovationen.
Neben den reinen Kostenvorteilen im Betrieb sehen weltweit Unternehmen und Organisationen des öffentlichen Bereiches den wesentlichsten Nutzen in den Auswahlmöglichkeiten unserer breiten Softwarepalette, welche industriespezifische Anwendungsfälle (SAP Industry Cloud) und ebenfalls Line-of-Business Produkte umfasst. Dies baut auf sicheren Plattformfähigkeiten auf, welche darüber hinaus die „Intelligenz", Automatisierung, User Experience und Erweiterbarkeit sicherstellen.
Die Anwendungen in einer Public Cloud stellen die rasche Implementierung von standardisierten Prozessen sicher, bei denen Kundinnen bzw. Kunden sich nicht differenzieren müssen, wie zum Beispiel Reisekostenmanagement mit



SAP Concur oder ähnlichen Anwendungen des Business Networks. Wir sehen allerdings ebenso Kundinnen bzw. Kunden als hybride Nutzer bzw. Nutzerinnen unseres Cloudangebotes an, also von Public und Private Cloud, auf der Grundlage eines einheitlichen Datenmodells, User Experience und Semantik.

In welchen Bereichen kommen Cloudsysteme im Behördenumfeld zum Einsatz?

Global zeichnet sich der Trend zum vermehrten Einsatz von Cloudsystemen im öffentlichen Dienst ab. Vor allem im Universitäts- als auch im Local-Bereich, zum Beispiel auf der Ebene der US Counties. Beide profitieren schon jetzt immens durch die zuvor erwähnten Vorzüge der Cloud und können somit ihren Mitarbeiterinnen bzw. Mitarbeitern, Studierenden und Bürgerinnen bzw. Bürgern ein verbessertes Serviceangebot liefern. Bei großen staatlichen Behörden steht initial der Betrieb von Private-Cloud-Systemen im Vordergrund. Man möchte die Vorteile von Cloudsystemen ebenso nützen, gleichzeitig gilt es hoheitliche Anforderungen zu erfüllen. Diese umfassen unter anderem die Themen Data Residency und Data Security, Betrieb, sowie den Software Lifecycle.
Generell geht es unseren Kundinnen und Kunden darum, dass Data Residency „in Region", „in Country" oder auch „at Customer" (HEC customer edition), mit „Compliant Operations" (EU Access) unterstützt werden. Diese Deployment-Methoden ermöglichen ebenfalls den Nutzen von Cloud Technologien für kritische Kernprozesse einer Behörde und somit auch dort mittelfristig Kosten und Risiken zu senken. Die SAP National Security Services sind dafür das beste Beispiel einer solchen Umsetzung.

In welcher Form sind Cloudsysteme auch in kritischen Anwendungsfällen im Behörden-Umfeld vermehrt einsetzbar?

Die Vorteile von Cloudsystemen sind auch für kritische Prozesse realisierbar, sobald die dafür notwendigen Sicherheitsanforderungen erfüllt sind. Dafür gibt es schon sehr gute Beispiele. So durchlaufen die National Security Services* der SAP international anerkannte Prozessstandards, welche die Anforderungen an das Informationsmanagement in Behörden widerspiegeln. Diese umfassen alle Layer einer Cloudarchitektur von der Infrastruktur, über die Plattform und zu den Applikationen. Je nach Komposition dieser kann man schon auf vorhandenen Zertifizierungen aufbauen oder muss die jeweiligen Sicherheitsüberprüfungen vollständig durchlaufen. Wir verfügen über eine eigene globale Einheit, ehemaliger CISOs und anderer Security und Secrecy Experten, welche exakt jene Anforderungen und Prozesse gemeinsam mit den Kundenansprechpartnern bewältigen. Die Kundenlandschaft ist an sich weitgefächert und umfasst neben den zu erwartenden Defense, Police und Intelligence Organisationen auch Smart Cities sowie andere öffentliche Einrichtungen.

„Global zeichnet sich der Trend zum vermehrten Einsatz von Cloudsystemen im öffentlichen Dienst ab."

* Details dazu sind abrufbar unter:
https://sapns2.com/security/

Wie realisiert SAP die Sicherheit der angebotenen Cloud-Dienstleistungen?

Ohne End-to-End Security geht es nicht. Vom Bereich des Product Engineerings angefangen, gilt es über den gesamten Softwarelebenszyklus „Security by Design“ sicherzustellen. Diese ganzheitliche Betrachtung umfasst ebenso die Organisation als auch die darin stattfindenden Abläufe. Zu diesem Zweck haben wir Prozesse installiert, die regelmäßig auditiert und zertifiziert werden, um End-to-End-Security auf technischer und auf organisatorischer Ebene zu sichern.

„Persönlich hoffe ich nicht, dass wir eine „Datenkolonie“ anderer werden.“

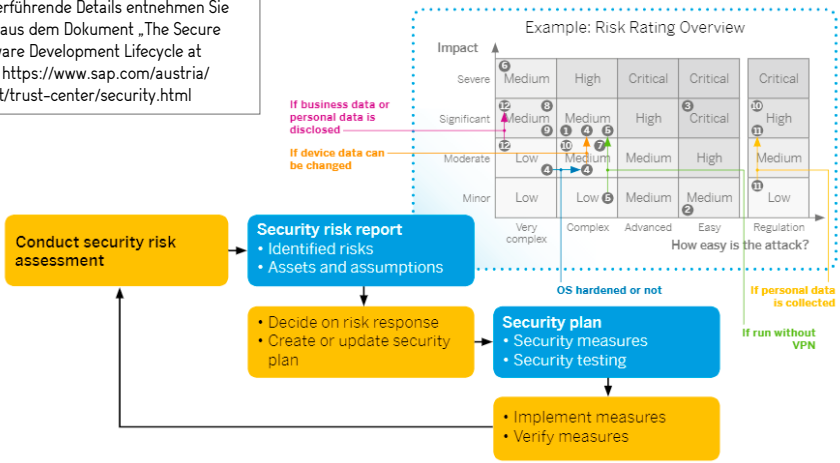
Bei Anwendungsfällen im Behördenumfeld oder der regulierten Industrie, wie zum Beispiel der militärischen Luftfahrt, arbeiten wir mit einer kontinuierlichen Risikoanalyse, mit dem Fokus auf Datenklassifizierung und Datensouveränität, um etwaige neue Anforderungen an die Schutzfunktionen zu erkennen.

Welche aufkommenden Entwicklungen und welche Trends sehen Sie insbesondere im Zusammenhang mit der digitalen Souveränität?

SAP hat die Wichtigkeit der digitalen Souveränität für unsere Kundinnen und Kunden erkannt. So setzt die SAP. als Gründungsmitglied von GAIA-X*, einem wegweisenden Projekt für die Gestaltung eines digitalen Ökosystems für Europa, langfristig auf den Einsatz sicherer sowie offener Technologien.
Die derzeitige Gesundheitskrise COVID-19 verdeutlicht die Abhängigkeit von Produkten aber auch von IT Services außereuropäischer Anbieter. Die Schaffung eines Systemverbundes zum sicheren und homogenen Datenmanagement, basierend auf gemeinsamen technischen Standards, ist sicherlich der richtige Schritt zur Sicherstellung einer europäischen digitalen Souveränität. Persönlich hoffe ich nicht, dass wir eine „Datenkolonie“ anderer werden.

* Auf dem Weg zu einer europä Cloud-und Dateninfrastruktur, https://www.dsag.de/gaia-x

Weiterführende Details entnehmen Sie bitte aus dem Dokument „The Secure Software Development Lifecycle at SAP“ https://www.sap.com/austria/about/trust-center/security.html



Cloud-Technologie

für die nächste Generation der Verwaltung

Im aktuellen Regierungsprogramm kommt das Wort „digital“ in diversen Kombinationen und Ausprägungen 194-mal vor. Natürlich ist dort auch Cloud ein wichtiges Thema. So soll etwa für alle Österreicher/innen eine sichere Ö-Cloud eingeführt werden und für den Public Sector eine Bundes-Cloud entstehen. Das BRZ beschäftigt sich schon seit einigen Jahren mit Cloud-Technologien. Speziell für die Verwaltung ist essenziell, dass für ihre Services und Anwendungen Cloud-Technologie on premise im BRZ aufgebaut wird. Nur so kann die Datenhoheit garantiert werden und gleichzeitig alle Vorteile dieser Technologie genutzt werden.

„Werden CI/CD Pipelines automatisiert, müssen auch die geltenden Sicherheitsrichtlinien automatisiert werden.“

Eine Ausprägung der Cloud-Technologie ist **Platform as a Service (PaaS)**. Das ist ein Cloud Computing-Modell, das eine Hard- und Software-Plattform für den gesamten Lebenszyklus von modernen, web-basierten IT-Anwendungen zur Verfügung stellt. Die PaaS-Plattform stellt flexibel nutzbare und skalierbare IT-Ressourcen, Mandantenfähigkeit und Zugriffskontrolle, integrierte Laufzeitumgebungen und gegebenenfalls auch Software-Entwicklungsumgebungen zur Verfügung.

Kurze Release Zyklen, dynamische Nutzung

Die Plattform interagiert dabei eng mit Umgebungen für Automatisierung wie Continuous Integration (CI) und Continuous Delivery / Continuous Deployment (CD) und unterstützt somit häufigere Code Änderungen, kurze Release Zyklen und eine dynamischere Nutzung der Infrastruktur. Die Einhaltung von bestehenden Sicherheitsrichtlinien und deren Überarbeitung oder Anpassung im Zusammenhang mit dieser Automatisierung ist unabdingbar. Werden CI/CD Pipelines automatisiert, müssen auch die geltenden Sicherheitsrichtlinien automatisiert werden.

Moderne Plattformen bauen auf einer Container as a Service Infrastruktur (CaaS) auf, wobei Kubernetes als Werkzeug zur Orchestrierung, Skalierung und Verwaltung der Container den de-facto Marktstandard darstellt. Das BRZ verwendet ebenfalls eine Enterprise-Lösung die auf Kubernetes basiert.

Effiziente und agile Software-Entwicklung

Neue Anwendungen werden im BRZ ausschließlich nach cloud-nativen

Architekturprinzipien agil entwickelt. Der Initialaufwand bei der Implementierung neuer Software-Projekte wird durch den Einsatz der PaaS zukünftig stark reduziert. Infrastruktur sollte automatisiert und konfigurationsbasiert instanziiert und bereitgestellt werden. Dadurch liegt der Fokus zur Gänze auf einer effizienten und agilen Anwendungsentwicklung.

Die Plattform ermöglicht zudem den gezielten Einsatz von Ressourcen. Hardware muss nicht exklusiv für dedizierte Anwendungen vorgehalten werden und Lastspitzen in Anwendungen können durch horizontale Skalierung der Services abgefangen werden. Das ermöglicht insgesamt eine effizientere Nutzung von Ressourcen bei gleichzeitiger hoher Verfügbarkeit.

„Neue Anwendungen werden im BRZ ausschließlich nach cloud-nativen Architekturprinzipien agil entwickelt."

Kostenreduktion im Fokus

Im Zusammenspiel mit Cloud-native Applikationen bietet die PaaS eine Near Zero Downtime-Plattform. Zusätzlich bietet die PaaS eine Plattform und Methoden zur schrittweisen Modernisierung von älteren IT-Anwendungen. Bei richtigem Einsatz kann der Einsatz dieser Technologie zu einer Kostenreduktion sowohl im Bereich Software-Entwicklung als auch im Betrieb führen.

Mag. Clemens Schwaiger

Bundesrechenzentrum (BRZ)
Product Management, Digital Advisory

Stärkung der Cyber-Resilienz im Behördenumfeld durch Kooperation auf einer Vertrauensbasis

Wenn wir in Österreich von Cyber-Security und Cyber-Resilienz reden, müssen wir beides als ein Thema begreifen, das uns alle betrifft. Jede in Österreich lebende Person, jedes Unternehmen und jede Behörde ist im Lebens- und Arbeitsalltag auf digitale Dienste und Infrastrukturen angewiesen. Die Abhängigkeit steigt tendenziell immer stärker, gleichzeitig eröffnen sich mehr und mehr Angriffsmöglichkeiten. Cyber-Security muss daher als gemeinschaftliche Aufgabe wahrgenommen werden, die uns alle angeht. Gerade das Bundeskanzleramt (BKA) nimmt im Bereich der Cyber-Security eine Rolle als zentrale Schnittstelle des Staates zu Gesellschaft, Wirtschaft und Wissenschaft ein und schafft den organisatorischen Rahmen für die Zusammenarbeit der Akteure. In diesem Sinne setzt das Büro für strategische Netz- und Informationssystemsicherheit (strategisches NIS-Büro), welches im BKA als Teil der Abteilung I/8 angesiedelt ist, stark auf die öffentlich-private Zusammenarbeit. Durch das NIS-Gesetz wurden etwa Computer-Notfallteams (CERTs) erstmals gesetzlich verankert und die operative Zusammenarbeit sowohl zwischen den Cybersicherheitsbehörden als auch mit den CERTs auf eine rechtlich gesicherte Basis gestellt. Auf diese Weise konnte die operative Zusammenarbeit verbessert und das Lagebild weiter verfeinert werden. Die Ermittlung der Betreiber wesentlicher Dienste durch das strategische NIS-Büro erhöht zudem unmittelbar das Cybersicherheitsniveau kritischer Infrastrukturen, die für die Daseinsvorsorge in Österreich von Bedeutung sind. Hierbei kann auch das Österreichische Informationssicherheitshandbuch als Grundlage einer risikobasierten Verbesserung der Informationssicherheit von den Betreibern wesentlicher Dienste herangezogen werden. Künftig wird darüber hinaus dem Bereich der Forschung und Entwicklung und dem strukturierten und durchlässigen Wissensaustausch zwischen Wissenschaft, Forschung, Wirtschaft und Verwaltung steigende Bedeutung zukommen. Das BKA und das strategische NIS-Büro werden den Kurs der öffentlich-privaten Zusammenarbeit weiter fortsetzen und vertiefen, um die gemeinschaftliche Aufgabe der Cyber-Security und die Herausforderungen interdisziplinär und übergreifend zu adressieren.

> *„Das NISG fördert die Verbesserung der Cyber-Sicherheit in Österreich durch die Umsetzung der NIS-Richtlinie und die Ermöglichung eines kooperativen Informationsaustauschs als Erfolgskriterium für die Stärkung der Cyber-Security in Österreich."*
>
> *Mag. Vinzenz Heußler*

Mag. Vinzenz Heußler, LL.M.

Leiter des strategischen NIS-Büros
Abteilung I/C/8 – Cyber Security, GovCERT, NIS-Büro und ZAS

NISG – Nachhaltiges Stärken eines hohen Niveaus für die Informationssicherheit in Österreich

Der Kern des Ende 2018 umgesetzten Netz- und Informationssystemsicherheitsgesetz (NISG) ist die Sicherstellung jener Dienste, die für die österreichische Bevölkerung wesentlich sind. Das Gesetz richtet sich daher an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste (z.B. Online-Marktplätze, Suchmaschinen und Cloud-Computing-Dienste) und Einrichtungen der öffentlichen Verwaltung. Die Betreiber wesentlicher Dienste sind Einrichtungen aus den Bereichen Energie, Verkehr, Finanzmarktinfrastruktur, Bankwesen, Trinkwasserversorgung, Gesundheitswesen und digitale Infrastruktur.

Diese Betreiber sind verpflichtet, Sicherheitsvorfälle zu melden und Sicherheitsvorkehrungen zu treffen. Alle drei Jahre sind diese Vorkehrungen dem BMI gegenüber nachzuweisen, wobei das BMI ermächtigt ist, dies an Ort und Stelle nachzuprüfen. Bei Auftreten eines Sicherheitsvorfalles müssen die Betroffenen eine Meldung unverzüglich an das zuständige Computernotfallteam erstatten, welches die Meldung im Falle einer Pflichtmeldung an das BMI weiterleitet. Neben der Funktion als Informationsdrehscheibe liegt der Schwerpunkt eines Computernotfallteams darin, erste Hilfe zu leisten und bei Notfallmaßnahmen zu unterstützen.

Der Notwendigkeit einer engen Kooperation auf staatlicher Ebene wurde im NISG ebenfalls Sorge getragen.

Im Rahmen des IKDOK (Innerer Kreis der Operativen Koordinierung) treten Vertreter des BMI, BKA, BMLV und BMEIA periodisch und anlassbezogen zusammen. In der Opkoord kommen der IKDOK, die Computernotfallteams sowie Vertreter von Unternehmen zusammen.

Durch das NISG wird zwar nur eine kleine Anzahl von Unternehmen direkt reguliert; da allerdings auch die Lieferkette in die Bewertung der Sicherheitsmaßnahmen miteinfließt, kann man davon ausgehen, dass die Thematik Cyber-Sicherheit auch weit über die unmittelbar dem NISG unterliegenden Firmen hinaus an Bedeutung gewinnt. Das NISG ist somit ein erster wichtiger Schritt, um das Thema Cyber-Sicherheit in einen gesetzlichen Rahmen zu gießen.

DI Philipp Blauensteiner, MA
Gf. Leiter der Abteilung Cyber-Sicherheit

Mag. Gernot Goluch
Leiter des NIS-Referats
BVT

Webshop, Home-Office & Ö-Cloud

Standbeine für einen erfolgreichen Standort Österreich

Österreich ist längst in der digitalen Welt angekommen. Konsumentinnen und Konsumenten nutzen das Web beinahe zu 100 % für Kaufentscheidungen. Computer und Smartphone gehören zum Alltag, doch Unternehmen in Österreich fällt es nicht immer leicht, mit diesen digitalen Entwicklungen mitzuhalten. Wie eine Studie von Arthur D Little aus dem Jahr 2019 zeigt, hat der Digitalisierungsgrad der heimischen Unternehmen noch Luft nach oben.

Es zeigt sich aber im Vergleich mit 2018 und 2017 eine klare Tendenz in die richtige Richtung. So fand sich 2018 noch ein Großteil der Unternehmen in den Kategorien „digitaler Neuling" oder „digital bewusst" wieder. 2019 bewegte sich ein zunehmender Anteil in Richtung „digital bewusst" oder „digital orientiert". Knapp 10 % der befragten KMU befanden sich 2019 in den Kategorien „digital orientiert" und „digitaler Champion".

Covid-19 als Katalysator für die Digitalisierung

Nicht zuletzt hat Covid-19 zu einem neuerlichen Digitalisierungsschub geführt. Diese Krise hat den Umschlagplatz heimischer Betriebe in die digitale Welt verlagert und gezeigt: Digitale Prozesse und Plattformen sind Erfolgsfaktoren für die Zukunft. Mit dem Umsatzwegfall, ausgelöst durch das Fehlen der Laufkundschaft, waren österreichische Betriebe gezwungen, Produkte und Dienstleistungen von einem Tag auf den nächsten ins Netz zu verlegen. Unzählige Webshops wurden über Nacht eingerichtet, um in Zeiten von Corona-Lockdowns und Ladenschließungen zumindest digital wirtschaften zu können.

> „Die aktuelle Krise hat den Umschlagplatz heimischer Betriebe in die digitale Welt verlagert und gezeigt: Digitale Prozesse und Plattformen sind Erfolgsfaktoren für die Zukunft."

Die aktuelle Lage macht die Implementierung dieser Prozesse oft kompliziert und schwierig. Hier setzen die UBIT-Mitgliedsbetriebe an: Sie unterstützen professionell und rasch bei der technischen Umsetzung und beim Aufbau der starken Online-Präsenz. Ein digitales, krisensicheres Standbein zu haben ist jedenfalls empfehlenswert, wenn nicht gar notwendig. Diese Betriebe haben jetzt und in Zukunft wesentliche Vorteile.

Home-Offfice erfordert verstärkte Cybersicherheit

Doch nicht nur Produkte und Dienstleistungen wurden ins Netz verlegt, die aktuelle Situation hat zahlreiche heimische Unternehmen dazu veranlasst, ihren Betrieb in die Heime ihrer Mitarbeiter und Mitarbeiterinnen zu verlagern. Diese Tatsache bringt viele neue Herausforderungen mit sich, u.a. besondere Sicherheitsrisiken. Ungeschützte oder schlecht abgesicherte IT-Infrastruktur erleichtert es Online-Betrügern und Hackern, aus

der Krisensituation Profit zu schlagen. Gefahr geht insbesondere von Phishing-E-Mails und unsicheren Links aus.

Unternehmerinnen und Unternehmer sollten sich daher die Frage stellen: „Ist mein Unternehmen ausreichend geschützt?“ Die österreichischen IT-Dienstleistungsunternehmen leisten hier wichtige Unterstützungsarbeit, um den Betrieb über Home-Offices zu gewährleisten und Gefahren abzuhalten – allen voran die zertifizierten „Data & Security Experts“ (Details sind auf S. 94 zu finden).

Auch die unternehmenseigenen Beschäftigten über Cybersicherheit zu informieren, ist besonders jetzt von größter Bedeutung.

IT-Lösungen aus Österreich bündeln

Der nächste Schritt in diesem Prozess ist ein eigener IT-Cluster rund um österreichische Leitbetriebe. Wir sollten uns bei der Speicherung sensibler Daten unabhängiger von Anbietern aus den USA oder Asien machen. Digitalisierungsministerin Margarete Schramböck hat die Schaffung einer eigenen „Ö-Cloud“ angeregt, gemeinsam mit heimischen Rechenzentren-Betreibern, um die digitale Souveränität Österreichs herzustellen. An Bord der Cloud-Allianz sind Unternehmen wie A1, A-Trust, Anexia, das Bundesrechenzentrum und Kapsch. Ziel ist die Schaffung einer nationalen Infrastruktur, auf der Nutzerinnen und Nutzer Daten im Inland speichern können. Die Ö-Cloud ist eine wichtige Initiative für mehr Rot-Weiß-Rot in der IT-Branche. Mit diesem IT-Cluster können wir österreichische Lösungen gemeinsam fördern.

„Die Ö-Cloud ist eine wichtige Initiative für mehr Rot-Weiß-Rot in der IT-Branche. Es gibt die Idee, rund um heimische Leitbetriebe einen ganzen IT-Cluster zu formen, um österreichische Lösungen gemeinsam zu fördern. Wir müssen mehr Bewusstsein für IT aus Österreich schaffen.“

Wir müssen mehr Bewusstsein für IT aus Österreich schaffen. Damit stärken wir Österreich als Digital- und Wirtschaftsstandort nachhaltig.

KR Mag. Alfred Harl, MBA CMC
Obmann des Fachverbandes UBIT
der WKO

Blockchain & Security-Management

DAS JOSEF-RESSEL-ZENTRUM FÜR BLOCKCHAIN-TECHNOLOGIEN & SICHERHEITSMANAGEMENT

Wegen ihrer Rolle für innovative Finanzprodukte und bei Kryptowährungen haben Blockchain-Technologien zuletzt viel Aufmerksamkeit erregt. Auch werden immer wieder weitere Anwendungsfelder für diese Technologie in den Raum geworfen. Umfasst ist davon etwa die Nutzung als dezentraler und besonders fälschungssicherer Datenspeicher z.B.: für Banken, Kapitalmärkte, Notare, bzw. Lebensmittellieferketten.

Klassische, sichere IT-Systeme stellen aber grundlegend andere Anforderungen an eine Technologie als Kryptowährungen. Ein wesentlicher Aspekt bei der Nutzung von Blockchains liegt dabei in der Bereitstellung geeigneter Zugriffskontrollen: Zugang auf Informationsbestandteile muss feingranular gewährleistet und an Nutzer und/oder Rollen gebunden werden können. Bei Kryptowährungen ist das anders, nämlich möglichst von allen lesbar. Dieser Zugriffsschutz wird auch durch Regularien (z.B.: DSGVO) gefordert, aber der Zugang muss auch entziehbar sein. Ein weiterer Aspekt bei der Erstellung sicherer Systeme liegt im Security-Management: Wie sieht die Management-Perspektive der Security von Blockchains aus, wie sind IT-Sicherheitsstandards anzupassen und wie geht man um mit Angriffen und Incidents wie etwa Angriffe auf die Implementierung eines Systems, Fraud oder die Einbringung illegaler Inhalte in eine Technologie, deren wesentliches Merkmal in der Nichtveränderbarkeit der Inhalten liegt. Auch ist sicherzustellen, dass die zuständigen Programme unverändert und unverfälscht ausführbar sind. Das bedingt eine enge Verzahnung mit dem Themenbereich des Trusted Computings.

„Ein weiterer Aspekt bei der Erstellung sicherer Systeme liegt im Security-Management“

Das JR-Zentrum fokussiert sich auf die Erforschung und Entwicklung von Grundlagentechnologien zur Nutzung und Integration von Blockchains in klassische IT-Systeme. Die Forschungsaspekte umfassen technische Grundlagenforschung im Bereich der angewandten Kryptographie und auch das Security-Management für Blockchain-basierten Anwendungen, bzw. die sicheren Integration von Blockchains in klassische Systeme.

Big Data Analytics

ERFORSCHUNG VON METHODEN ZUR AUSWERTUNG GROSSER DATENMENGEN UNTER WAHRUNG VON PRIVACY- UND DSGVO-ANFORDERUNGEN

Dank der fortschreitenden Digitalisierung vieler Arbeits- und Lebensbereiche und damit verbundenen Möglichkeiten in Bezug auf neue Produkte und Dienstleistungen hat Privacy an Bedeutung zugelegt. Trends wie personalisierte Dienstleistungen und Produkte, die sich oft durch den Verkauf von personalisierter Werbung, oder gar der Kundendaten finanzieren, sind in den Brennpunkt gerückt. Auch wurde dank der europäischen General Data Protection Regulation (GDPR) der Datenschutz gestärkt. Seit Mai 2018 ist die in Österreich umgesetzte DSGVO in Kraft.

Den Datenschutzbemühungen stehen eine Vielzahl von Interessen in Forschung und Wirtschaft gegenüber, die auf der Bereitstellung personenbezogener Daten beruhen. Deren Datenqualität ist oft wesentlich. Die Forschung zeigte, dass Anonymisierungsverfahren im Allgemeinen stark verzerren. Das wirkt sich auf die Datenqualität aus. Die bisher als Ersatz genutzte Pseudonymisierung ist gem. DSGVO nicht mehr als geeignete Schutzmaßnahme einsetzbar.

In diesem Projekt werden Methoden erforscht, negative Effekte auf die Ergebnisse von Big-Data-Analysen abzuschätzen und einzudämmen. Dabei sind verschiedene Rahmenbedingungen zu beachten, je nachdem ob es sich um Trendanalysen, oder exakte Auswertungen handelt.

Ein wichtiger Aspekt der DSGVO ist die informationelle Selbstbestimmung: Dazu gehört das Recht der nachträglichen Rücknahme der Zustimmung, sowie das Recht auf Transparenz und letztlich das Recht auf Datenlöschung. Datensubjekte haben das Recht auf Auskunft, welche ihrer Daten wofür verwendet werden. Prozesse müssen dies berücksichtigen. Das ist eine komplexe Herausforderung im Hinblick auf intelligente Algorithmen. Demzufolge werden in diesem Projekt Methoden entwickelt um Transparenz zu gewährleisten, ohne dadurch neue Datenschutzgefahren zu generieren, sowie Methoden zur Datenlöschung aus komplexen IT-Systemen.

DI Peter Kieseberg

Institutsleiter
Institut für IT Sicherheitsforschung
Josef-Ressel-Zentrum

Die Vorteile eines zertifizierten ISMS

MEHRWERT FÜR KUNDEN UND UNTERNEHMEN

Mit einem Information Security Management System (ISMS) kann der Schutz der Informationen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit in einer Organisation gemanagt werden.

Die ISO27001-Norm, nach der das ISMS im BRZ aktuell zertifiziert ist, bietet einen Katalog von sogenannten Security-Controls, die den Schutz in mehreren Dimensionen abbilden. Das inkludiert die technischen Sicherheitsmaßnahmen in IT-Systemen, die Maßnahmen zur Bereitstellung einer sicheren Infrastruktur von der Zutrittskontrolle bis zur Ausfallsicherheit der Stromversorgung, die Regeln für die Benutzer/innen zur sicheren Verwendung der Informationen, vor allem aber die Regeln für die Administratorinnen/Administratoren der IT-Systeme für einen sicheren Umgang mit den dort verarbeiteten Informationen.

Ein Mehrwert für unsere Kunden

Für Kunden eines IT-Dienstleisters ist diese Abschätzung des Risikopotenzials ein geeigneter Maßstab für die Bemessung der Security-Maßnahmen, die zum Schutz der Informationen aufgewendet werden sollen. Zahlreiche Maßnahmen bietet ein zertifizierter IT-Dienstleister bereits standardmäßig an, sodass Kunden für Leistungen mit normalem Schutzbedarf ohne den Aufwand einer umfassenden, detaillierten Analyse bereits ein angemessenes Sicherheitsniveau in den Produkten vorfinden.

„Mit der Zertifizierung eines IT-Dienstleisters erhält dessen Kunde eine von unabhängiger Stelle geprüfte Bewertung des Dienstleisters."

Mit der Zertifizierung eines IT-Dienstleisters erhält dessen Kunde eine von unabhängiger Stelle geprüfte Bewertung des Dienstleisters und die Bestätigung, dass die international akzeptierten Sicherheitsregeln ordnungsgemäß umgesetzt werden. Damit steht für den Auftraggeber die Bestätigung zur Verfügung, dass er sich im Rahmen seiner Vergabe der Leistungen von der ordnungsgemäßen Handhabung der allgemein gültigen Sicherheitsregeln überzeugt hat und diese Bestätigung auch regelmäßig weiter geprüft wird.

> *Bestrebungen einer Organisation sollten im Idealfall über die Anforderungen für eine Zertifizierung hinausgehen. Ziel jeder Organisation sollte immer ein bestmöglicher und ganzheitlicher Umgang mit dem Thema IT-Sicherheit sein, sodass Anforderungen aus Zertifizierungsstandards automatisch erfüllt sind."*
>
> Dr. Thomas Zefferer, Senior IT-Security Expert A-SIT Plus GmbH

Ein Mehrwert für das Unternehmen

Mit der Einrichtung eines ISMS ist die Analyse und Bewertung der Risiken für die Sicherheit der Informationen untrennbar verbunden. Dabei stellt die Betrachtung der IT-gestützten Informationsverarbeitung einen wesentlichen Teil der Aufgabe dar. Informationen liegen jedoch nicht nur als Daten in IT-Systemen vor, sondern sie existieren auch in gedruckter Form auf Papier oder als gesprochene Worte, die ebenso in diese Betrachtung einzubeziehen sind.

Dieser ganzheitliche Ansatz, der vor allem auch die Menschen, die mit den Informationen arbeiten, in das Sicherheitskonzept einbezieht, ist ein wichtiger Grundsatz. Zahlreiche Angriffe auf die Informationssicherheit erfolgen heute in Kombination zwischen einem technischen Angriffsvektor (Schad-Software) und einem Angriff auf den User, der dazu verleitet werden soll, vorhandene Sicherheitsmechanismen zu umgehen. Daher stellt die Awareness-Bildung bei den Usern von Informationen eine wesentliche Säule des BRZ-Sicherheitskonzepts dar.

Die Integration von Sicherheitsvorgaben in die Arbeitsabläufe des Alltags der Mitarbeiter/innen, die in ihrem Workflow neben der Erledigung ihrer Aufgabe auch die notwendigen Sicherheitsmaßnahmen setzen, macht die Informationssicherheit zu einem selbstverständlichen Bestandteil in den Unternehmensprozessen.
Diese Strategie führt schließlich dazu, dass jede/r Mitarbeiter/in eines Unternehmens auch ein/e Sicherheitsmitarbeiter/in ist.

Ing. Johannes Mariel

Bundesrechenzentrum (BRZ)
Abteilungsleiter Information Security

Moving Target Defense für Cloud Systeme

STÄNDIGES VERÄNDERN DES AUFENTHALTSORTS VON DATEN

Ein Dilemma der Systemsicherheit ist ihre asymmetrische Wahrnehmung: im besten Fall bemerkt man Sicherheitsmaßnahmen überhaupt nicht, im schlechtesten Fall erleidet man den maximal möglichen Schaden, der durch nicht funktionierende oder nicht vorhandene Security entstanden ist.

Gleichermaßen besteht oft Argumentationsdruck: Wofür braucht man Security, wenn derzeit alles gut läuft? Wieso dafür bezahlen, dass ein Service der augenscheinlich gut läuft auch weiterhin gut läuft?
Security erzeugt typischerweise keinen Return-of-Investment, sondern wendet lediglich Schaden ab, weswegen eine Quantifizierung des Nutzens in der Praxis bisweilen schwierig ist. Hier bietet die Forschung im Bereich der spieltheoretischen Sicherheit/Security Economics neue Ansätze: Ziel ist es, Angriffe nicht auszuschließen, sondern mit den vorhandenen Ressourcen möglichst „teuer" für den/die Angreifer/in zu machen; im Idealfall teurer als der aus dem Angriff entstehende Nutzen.

Security Economics lässt sich etwa im Umfeld des Cloud Computing durch dynamische Datenverlagerung nach dem Zufallsprinzip umsetzen. Bei einer sogenannten „Moving Target Defense" wechselt das Ziel, d.h. die Daten in der Cloud, ständig ihren Aufbewahrungsort. Somit werden die Daten zum „beweglichen Ziel", was Angriffe i.A. erschwert.

Für Anbieter von Cloud Services bedeutet Security Economics die optimierte Umsetzung von Sicherheitsmaßnahmen auf eine von zwei Arten: welche Mechanismen sind innerhalb des gegebenen Budgets realisierbar, um die Sicherheit zu maximieren? Oder alternativ: Wie sieht die kostengünstigste Option aus, eine geforderte Mindestsicherheit zu etablieren? Optimierungs- und Spieltheorie stellen hierbei neue Werkzeuge für einen ökonomischen Zugang zur Systemsicherheit dar, ergänzend zu klassischen Mitteln der Kryptographie.

Assoc. Prof. DDipl.-Ing. Dr. Stefan Rass

Assoziierter Professor
Institut für Angewandte Informatik
der Alpen-Adria-Universität Klagenfurt
(Cyber-Security Group, Semantic Systems Group)

TOPIC 2

Digitale Identitäten

Mobile Security

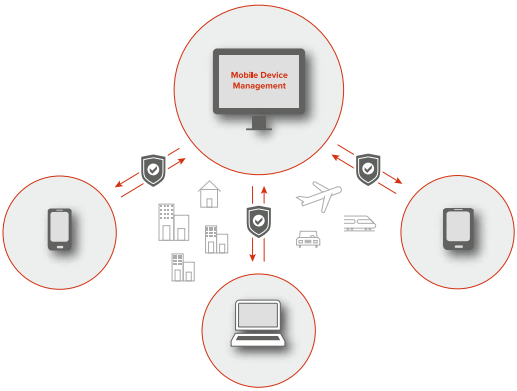
Lückenloser Datenschutz dank Mobile Device Management

Mobiles Arbeiten ist vielen Unternehmen ein Anliegen. Ob Außendienst oder Dienstreise, der Wunsch nach mehr Flexibilität oder einfach die zusätzliche Nutzung von Smartphones und Tablets – die mobilen Betriebssysteme haben längst Einzug in unsere Arbeitswelt gehalten.
Während Workstations und Serverlandschaften meist über erprobte Sicherheitsvorkehrungen und homogene Betriebssysteme verfügen, kommt es bei mobilen Endgeräten gerne zu Mischformen. Auch darüber hinaus steht die IT vor neuen, teils komplexen Herausforderungen – beginnend damit, dass mobile Geräte schwieriger zu überblicken sind und dass teils firmenfremde Geräte auf Unternehmensdaten zugreifen.

„Ohne Hilfe eines MDM sind die Anforderungen der DSGVO nur schwer zu erfüllen."

Sicherheit und Kontrolle über Daten, Apps und Berechtigungen

Ohne Hilfe eines MDM (Mobile Device Management) sind die Anforderungen der DSGVO nur schwer zu erfüllen. Sensible Informationen wie Kontaktdaten oder E-Mails sind auch auf Laptops, Smartphones oder Tablets vor Fremdzugriffen und Verlust zu schützen. Die Geräte müssen passwortgeschützt sein und über einen Virenschutz verfügen. Daten sind zu verschlüsseln, private und berufliche Informationen strikt zu trennen. Zudem muss sichergestellt werden, dass via App-Berechtigungen keine Gefahren für



die Sicherheit sensibler Daten vorliegen, beispielsweise indem Social Media-Apps Zugriff auf Kontaktdaten erhalten.
Die Wahl der geeigneten Maßnahmen liegt beim Unternehmen selbst, ebenso der Selbsttest auf Effizienz und Vollständigkeit der Sicherheitsvorkehrungen. Professionelle MDM-Systeme decken alle Anforderungen zuverlässig ab. Die IT profitiert außerdem von der detaillierten Übersicht über alle mobilen Geräte mit Zugriff auf Unternehmensressourcen, inklusive der Möglichkeit, verlorene Geräte zu orten, zu sperren und auf Werkseinstellungen zurücksetzten. Geräte wie Applikationen können zentral verwaltet, aktualisiert und inventarisiert werden, auch wenn sie nicht vor Ort sind. So ist trotz strikter Vorgaben sicheres mobiles Arbeiten möglich.

Josef Pichlmayr
CEO
IKARUS Security Software GmbH

A-SIT TIPP

TOP-10 TIPPS

SMARTPHONE-SICHERHEIT DURCH MDM

- › Geschützte Umgebung
- › Smartphone-Plattform
- › Policies durchsetzen
- › App-Schutz
- › Trennung der Daten
- › Schutz vor Schadsoftware
- › Schutz der Übertragungskanäle
- › Sichere Pushnachrichten
- › Update-Management
- › Zugriffsschutz

Weitere Informationen sind abrufbar:
www.sicherheitshandbuch.gv.at/

Mobile Security

MÖGLICHKEITEN UND HERAUSFORDERUNGEN DES EINSATZES SICHERER HARDWARE-ELEMENTE IN MOBILEN ANWENDUNGEN

Mobile Betriebssysteme implementieren vielzählige Sicherheitsfunktionen, die in Desktop-Betriebssystemen nach wie vor nicht vorhanden sind, bzw. erst nach der Einführung in deren mobilen Pendants auch in klassischen Betriebssystemen ergänzt wurden. Beispiele dafür sind Sandboxing-Mechanismen, die Applikationen voneinander abschotten, der Einsatz von Hardware-Elementen für die sichere Ausführung von kryptographischen Operationen oder auch der mannigfaltige Einsatz von signiertem Code, der sowohl die Integrität des Betriebssystems als auch jene der installierten Applikationen sichert. Trotz dieser prinzipiell positiven Entwicklungen existieren auch im Bereich Sicherheit nach wie vor diverse Herausforderungen, die im Speziellen mobile Systeme, jedoch zu einem gewissen Grad auch andere IT-Systeme betreffen.

„Die Kryptographie stellt die technische Grundlage für das Absichern von Systemen dar."

Ein immer wiederkehrendes und nach wie vor nicht vollständig gelöstes Problem ist die mangelhafte Unterstützung kryptographischer Algorithmen durch sichere Hardware-Elemente mobiler Geräte. Die Kryptographie stellt die technische Grundlage für das Absichern von Systemen dar – im Konkreten um die Vertraulichkeit, die Integrität (und in weiterer Folge die Authentizität) von Daten zu garantieren. Vor allem auf mobilen Geräten ist die Anwendung kryptographischer Methoden unumgänglich für den Schutz verarbeiteter und gespeicherter Daten.

Sehr positiv ist in diesem Zusammenhang die Entwicklung zu sehen, dass in mobilen Geräten zunehmend sichere Hardware- (oder Hardware-nahe) Elemente für die sichere Ablage und Verwendung kryptographischer Schlüssel zur Verfügung stehen. So werden beim Entschlüsseln oder beim Signieren von Daten relevante Operationen direkt in diesen sicheren Hardware-Elementen ausgeführt, ohne dass der geheime Schlüssel diese sicheren Umgebungen verlässt bzw. aus diesen extrahiert werden kann. Die Wahrscheinlichkeit der Kompromittierung geheimer Schlüssel und der durch diese Schlüssel geschützte Daten wird dadurch signifikant reduziert. Heutige Geräte ermöglichen damit beispielsweise die Umsetzung sicherheitskritischer

Verfahren im Bereich Authentifizierung oder Ende-zu-Ende Verschlüsselung, die am klassischen Desktop in dieser Qualität nach wie vor nicht möglich sind. Weniger positiv ist allerdings, dass diese Hardware-Elemente trotz signifikanter Weiterentwicklungen in der Kryptographie auch heute noch nur ein sehr eingeschränktes Set lang bekannter kryptographischer Operationen unterstützen, die sich im Wesentlichen auf das Anwenden von klassischen asymmetrischen Signaturen (über die Algorithmen RSA und ECC) und symmetrischer Verschlüsselung (über AES) beschränken. Dies limitiert die Anwendung von Sicherheitstechnologien und damit auch das Anwendungsspektrum von mobilen Applikationen. Das volle Potential kryptographischer Verfahren bleibt damit ungenutzt.

Ziel muss es demnach sein, eine viel breitere Unterstützung von unterschiedlichen kryptographischen Operationen in sicheren Hardware-Elementen zu erreichen. Ein Beispiel dafür sind Proxy-Umschlüsselungsverfahren, bei denen eine Drittpartei Daten umschlüsseln kann, ohne diese Daten im Klartext zu kennen. Auch die Unterstützung spezieller Signaturverfahren, bei denen Teile der signierten Daten bewusst nachträglich geändert werden können ohne deren Signatur zu brechen, wären in diversen Anwendungsszenarien hilfreich. Schließlich sollte es auch das Ziel sein, für lang etablierte Verfahren im Bereich asymmetrischer Verschlüsselung, die trotz ihrer sonst weiten Verbreitung durch Hardware-Elemente nach wie vor nicht unterstützt werden (z.B. wird das ECDH-Verfahren für ECC-basierte asymmetrische Verschlüsselung von Hardware-Elementen aktueller Android-Geräte nicht unterstützt), eine entsprechende Unterstützung in sicheren Hardware-Elementen zu erreichen.
Zur Erreichung dieser Ziele sind hauptsächlich die Hersteller gefordert, da die jeweiligen Funktionen von den Betriebssystemen und den eingesetzten Hardware- und Software-Komponenten unterstützt werden müssen. Die (angewandte) Forschung kann hier jedoch durch das Vorantreiben von Standardisierungen, das Demonstrieren von Anwendungsgebieten, das Schaffen von Klarheit über die Sicherheit neuer Verfahren, das Bereitstellen von effizienten Demo-Implementierungen sowie das Auslagern von Algorithmen in Software bzw. entfernte Systeme für die Emulation von Verfahren entscheidend unterstützen. Durch Kooperationen von Forschungseinrichtungen und Herstellern kann eine Entwicklung vorangetrieben werden, die wesentlich zu einer sicheren Erschließung von neuen mobilen Anwendungsgebieten beitragen kann.

Dr. Peter Teufl
CEO
A-SIT Plus GmbH

A-SIT-CHECKLISTE

Handhabung komplexer Passwortsicherheit
Wie sind sichere Passwörter gestaltbar und verwendbar?

Weitere Details zu Passwörtern sind abrufbar unter:
www.onlinesicherheit.gv.at; www.sicherheitshandbuch.gv.at

ID	AKTIVITÄT	STATUS	
I	**PASSWORT-FESTLEGUNG**		
01	Auswählen starker und zufälliger Passwörter die schwer zu erraten sind	OK	KO
02	Im Idealfall Passwörter mittels geeigneter Hilfsprogramme automatisch generieren	OK	KO
03	Das Passwort soll Großbuchstaben enthalten	OK	KO
04	Das Passwort soll Kleinbuchstaben enthalten	OK	KO
05	Das Passwort soll Nummern enthalten	OK	KO
06	Das Passwort soll Sonderzeichen enthalten	OK	KO
07	Die Passwortlänge sollte dem Einsatzzweck angemessen sein, also mindestens neun Zeichen für Online-Dienste und entsprechend mehr für sensible Online-Dienste (z.B. solche mit personenbezogenen oder finanziellen Daten, Cloud-Dienste) und Offline-Anwendungen/-Verschlüsselung	OK	KO
08	Auswählen und festlegen zumindest einer Sicherheitsfrage, deren Antwort schwer zu erraten ist, um beispielsweise ein vergessenes Passwort wiederherzustellen; Frage und Antwort sind so zu wählen, dass niemand anders diese beantworten kann	OK	KO
09	Keine Standard-Passwörter oder gängige Kombinationen verwenden (z.B. 123456, passwort, qwertz, admin)	OK	KO
10	Keine persönlichen Details verwenden, die Dritten bekannt sein können (z.B. Name, Geburtsdatum, Adresse)	OK	KO
11	Keine Wörter verwenden die auch in einem Wörterbuch vorkommen, auch nicht mehrfach hintereinander	OK	KO
12	Keine direkten Referenzen oder Bezeichnungen für den jeweiligen Dienst im Passwort verwenden	OK	KO

II	PASSWORT-VERWENDUNG		
13	Passwort geheim halten	OK	KO
14	Passwort nur unbeobachtet eingeben	OK	KO
15	Passwort nur auf vertrauenswürdigen Geräten eingeben	OK	KO
16	Passwort nur für die jeweils vorgesehene Anwendung (z.B.: zuverlässige Webseite, Applikation) eingeben	OK	KO
17	Dasselbe Passwort nur für einen Anwendungsfall bzw. Dienst verwenden	OK	KO
18	Sperren von Computern bzw. anderen Geräten mit Benutzer-konten oder abschalten, wenn diese nicht genützt werden.	OK	KO
19	Abmelden von Webseiten wenn man diese verlässt (das Schließen der Webseite reicht nicht aus)	OK	KO
20	Keine Passwörter teilen bzw. versenden, insbesondere nicht über ungesicherte Kanäle (wie z.B.: E-Mail, Internet, Messen-ger-Dienste). Auch nicht bei einer Aufforderung	OK	KO
III	PASSWORT-MANAGEMENT		
21	Passwort-Manager verwenden zur Verwaltung der Passwörter und Zugangsdaten	OK	KO
22	Definieren starker Master-Passwörter für den Zugriff auf den Passwort-Manager	OK	KO
23	Passwort zeitnah ändern bei Kompromittierung oder Verdacht einer Kompromittierung eines Passworts (z.B.: unberechtigte Verwendung)	OK	KO
24	Passwörter nicht im Browser speichern; Ist das nicht vermeid-bar, sind diese zumindest durch ein starkes Master-Passwort zu schützen	OK	KO
25	Keinesfalls auf fremden Geräten Passwort-Dateien und darin hinterlegte Passwörter speichern	OK	KO
26	Passwörter nicht im Klartext aufschreiben und aufheben; Wenn dies trotzdem notwendig ist, dann nur in geschützter Form, sodass niemand anders davon weiß und darauf zugreifen kann	OK	KO
27	Passwort-Dateien nicht mit Dritten teilen bzw. austauschen	OK	KO
28	Änderung von Passwörtern ausschließlich durch Zeitablauf (z.B.: 1x pro Quartal) ist nicht mehr zeitgemäß	OK	KO

Digitale Transformation und Identität
Digitale Identitäten sind längst Alltag


© OSDAuer

Ing. Mag. Lukas Praml
CEO
Österreichische Staatsdruckerei GmbH

IT-Systeme werden komplexer. Industrie, Handel, Behörden und private Personen sind immer stärker durch Technologie vernetzt. Das Buzzword der „digitalen Transformation" hallt durch viele Branchen. Wie schlägt sich ein jahrhundertealtes Druckunternehmen in diesem Umfeld?

Das mit dem Buzzword kann ich vorbehaltlos unterschreiben. Das Problem liegt in der Unschärfe des Begriffs. Als Österreichische Staatsdruckerei sind wir ein gutes Beispiel dafür. Unser Unternehmen ist mehr als 215 Jahre alt und im Kern ein international renommierter Hochsicherheitsbetrieb für die Produktion von sicheren Identitätsdokumenten wie biometrischen Reisepässen und Führerscheinen. Die vielzitierte Digitale Transformation könnte für uns also bloß die Modernisierung und Digitalisierung des Herstellungsprozesses bedeuten. Das greift aber einfach zu kurz und deckt nicht einmal ansatzweise das enorme Potenzial ab, das hier schlummert.

Wo sehen Sie dann das größte Potenzial dieser Entwicklung?

In der Einfachheit, mit der wir die essenziellsten Teile unseres Lebens, unserer Identität, durch Digitalität sicher miteinander verbinden können. Und in der Möglichkeit, grenzüberschreitend zusammenzuarbeiten und gemeinsam diese Entwicklung voranzutreiben. Wir sehen den Trend hin zur Digitalisierung und digitalen Identitäten vor allem als Chance. 2017 hat die Staatsdruckerei genau aus diesem Grund mit der youniqx Identity AG ein hauseigenes Digital-Start up ins Leben gerufen.

Wir schützen Identitäten schon seit Jahrhunderten. Jetzt besteht unser Arbeitsmaterial aber nicht mehr nur aus Papier, sondern genauso auch aus Bits und Bytes. Mit erfolgreichen Launches unserer inhouse entwickelten elektronischen Identität „MIA" (My Identity App, Anm.) haben wir es geschafft, diese Einfachheit den Bürgerinnen und Bürgern zur Verfügung zu stellen. In Liechtenstein lassen sich damit seit heuer viele

Services der Liechtensteinischen Behörden per App nutzen, für die zuvor ein persönlicher Besuch notwendig war. Darüber hinaus haben wir mit MIA im Kosovo bereits erfolgreich den Führerschein digitalisiert per Smartphone zur Verfügung gestellt. Bei einer Verkehrskontrolle zücken Sie dort einfach ihr Smartphone, statt Führerschein oder Zulassungsschein. Womit wir wieder bei der Einfachheit wären.

Stichwort Einfachheit: Das Implementieren neuer Systeme ist ja oft keine einfache Aufgabe. Es gilt auf der einen Seite, die technischen Hürden zu meistern und andererseits auch den Enduser zufriedenzustellen. Sind Behörden und Bürger eigentlich gewillt, diesen Schritt zu wagen?

Definitiv. Das unterstreicht eine im September veröffentlichte Studie der EU deutlich. In den vergangenen zwei Jahren hat sich jedes der 36 teilnehmenden Länder bei seinen digitalen eGovernment-Services* verbessert. Natürlich kommt man da in einen Kreislauf. Mehr Angebot schafft mehr Nachfrage schafft mehr Angebot. Den deutlichsten Beweis dafür hat aber sicherlich die Corona-Pandemie erbracht. Die Bereitschaft zur Nutzung digitaler Werkzeuge im Berufs- und Privatleben ist hier für viele nicht mehr nur eine Frage der Bequemlichkeit, sondern eine dringende Notwendigkeit. Die Bürgerinnen und Bürger sind also auf jeden Fall bereit für den nächsten Schritt hin zur digitalen Identität.

Das birgt natürlich Risiken. Sicherheitslücken, Hacks, Zero-Day-Exploits: Wie können sich Behörden, Unternehmen und Bürger vor so abstrakten Bedrohungen schützen?

Durch Vertrauen. Das klingt nach einer Floskel, trifft aber genau den Kern. Ohne fundiertes Fachwissen ist ein effektiver Selbstschutz vor diesen diffusen Bedrohungen für den Durchschnittsbürger fast unmöglich. Man setzt sein Vertrauen in bestimmte Anwendungen und speziell darauf, dass diese auch entsprechend geschützt sind. Vertrauen ist eine extrem harte Währung und lässt sich nur langsam und mit viel Aufwand erarbeiten. Man ist als Sicherheitsunternehmen also ständig in der Pflicht, dieses Vertrauen Tag für Tag unter Beweis zu stellen. Deshalb steht

*Quelle: https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2020-egovernment-works-people

für uns die Sicherheit über allem. Diesen Grundsatz haben wir schon als analoges Sicherheitsunternehmen hochgehalten. Er ist auch die unumstößliche Grundlage bei unseren digitalen Identitätslösungen. Panzertüren, elektronische Türschlösser und Videokameras helfen hier wenig. Es braucht dynamische und durchdachte Sicherheitsansätze, die im Zentrum der gesamten Entwicklung stehen, sprich „security by design" und „security by code".

Sie sehen Sicherheit also weniger als einzelne Maßnahme und eher als ein Mindset?

Absolut. Bei uns steht dieses Thema ab Tag eins im Zentrum der Entwicklung. Das Ziel ist, den User und seine persönlichen, hochsensiblen Identitätsdaten bestmöglich zu schützen. Und zwar so, dass er gleichzeitig möglichst wenige Einschränkungen in Kauf nehmen muss. Unsere elektronische ID „MIA" speichert beispielsweise keinerlei persönliche Daten auf dem Smartphone des Users. Falls das eigene Gerät gestohlen oder verloren wird, muss man sich keine Sorgen um Identitätsdiebstahl machen. Die User merken von diesen Sicherheitsvorkehrungen im Normalfall nichts. Sie können ihre MIA-App im Alltag problemlos nutzen und sind dennoch geschützt. Darüber hinaus setzen wir natürlich auf moderne Sicherheitslösungen wie zum Beispiel den FIDO-Standard als sichere Authentifizierungsmöglichkeit.

Mit welchen Entwicklungen rechnen Sie in den kommenden Jahren im Bereich digitaler Identitäten?

Sie werden das Zentrum unseres Alltags sein. Digitale Identitäten sind schon heute nicht mehr aus dem öffentlichen Sektor wegzudenken. Man muss diese Entwicklung nur weiterdenken. Wissen Sie, bei wie vielen elektronischen Diensten Sie sich alleine in den vergangenen Tagen angemeldet haben? Jede Authentifizierung mit Nutzername und Passwort lässt sich genauso durch eine digitale Identität auf Knopfdruck durchführen. Natürlich will man das nicht überall, Stichwort Anonymität. Aber meine Bank, ein Onlineversandhaus oder meine Versicherung müssen sehr wohl wissen, wer ich bin. Mit einer verifizierten digitalen Identität können Sie sich sicher und bequem anmelden, und das weltweit. Womit sich auch der Kreis schließt und wir wieder bei der Einfachheit gelandet sind.

APP TO DATE
IN SACHEN IDENTITY SECURITY.

MIA ist die My Identity App der YOUNIQX Identity AG.

Sie ermöglicht eine einfache und sichere Identifikation per Smartphone und vereint gleichzeitig sämtliche Ausweisdokumente vollkommen digital in einer einzigen Anwendung. So macht MIA digitale Identität zur Realität.

YOUNIQX
Ein Unternehmen der Österreichischen Staatsdruckerei

mia.at

eIDAS-Verordnung

A-SIT als Bestätigungs- bzw. Konformitätsbewertungsstelle

Österreich hatte mit dem Signaturgesetz früh eine Basis für elektronische Signaturen, mit Bürgerkarte und Handy-Signatur auch bald verfügbare Umsetzungen. Der daraus entstandene Bedarf technischer Prüfung der Komponenten war mit ein Grund, dass A-SIT gegründet wurde.

Mit der EU Verordnung „eIDAS" (für: „electronic identification and trust services") wurde die gemeinschaftsrechtliche Basis deutlich geändert, für sogenannte Vertrauensdienste schon ab Mitte 2016 wirksam, im Bereich elektronischer Identität zuerst ab Ende 2018 zu bemerken, mittlerweile zunehmend in österreichische Anwendungen integriert. Diese beiden Bereiche – Vertrauensdienste und elektronische Identität – sind, neben einer allgemeinen Bestimmung zur Zulässigkeit elektronischer Dokumente, die wesentlichen Neuerungen aus eIDAS.

In den Vertrauensdiensten bringt eIDAS als EU-Verordnung, die für Mitgliedsstaaten direkt gilt, ein hohes Maß an Harmonisierung. Anwenderinnen und Anwender elektronischer Signaturen werden davon aber nur wenig bemerken: Eine qualifizierte elektronische Signatur erfüllt wie bisher das Erfordernis der Schriftlichkeit und ist der handschriftlichen Unterschrift rechtlich gleichgestellt. Die Neuerungen aus eIDAS betreffen vornehmlich Vertrauensdiensteanbieter und deren staatliche Aufsicht im Beginn und laufenden Betrieb der Dienste, sowie Hersteller von Komponenten. Was eIDAS neu einführt, sind eine Reihe weiterer Vertrauensdienste. Dies sind elektronische Siegel als Signatur der nicht-natürlichen Person, Validierungs- oder Bewahrungsdiente für Signaturen und Siegel, Zeitstempeldienste, Zustellung elektronischer Einschreiben und Zertifikate für Webseiten. eIDAS regelt deren EU-weite Anerkennung, es gibt zu einigen dieser neuen Vertrauensdienste auch österreichische Anbieter. Breitere Bedeutung in Österreich haben aber weiterhin die elektronische Signatur sowie neu für die Amtssignatur elektronische Siegel.
Ein neues Element in eIDAS ist die elektronische Identität, also die sichere Anmeldung an Online-Diensten. Dies aus eIDAS jedoch weniger stark harmonisiert als Vertrauensdienste und in weitgehender Verantwortung der Mitgliedsstaaten. eIDAS regelt die Interoperabilität und grenzüberschreitende Anerkennung. Anwenderinnen und Anwender von E-Government Diensten in Österreich bemerken dies, da seither neben dem Anmelde-Button für die Handy-Signatur oft ein Link oder Button „EU-Login" erscheint. Hintergrund ist die Verpflichtung, jene elek-

„In den Vertrauensdiensten bringt eIDAS als EU-Verordnung, die für Mitgliedsstaaten direkt gilt, ein hohes Maß an Harmonisierung."

tronischen Identitäten spätestens nach einem Jahr in Anwendungen öffentlicher Organisationen anzuerkennen, die andere Mitgliedstaaten auf entsprechenden Sicherheitsniveaus notifiziert haben. Mit Frühjahr 2020 haben schon Belgien, Dänemark, Deutschland, Estland, Kroatien, Italien, Lettland, Litauen, Luxemburg, Niederlande, Portugal, Slowakei, Spanien, Tschechien und das Vereinigte Königreich ein elektronisches Identifizierungsmittel notifiziert. Einige davon sind bereits im österreichischen System verfügbar, weitere werden im Verlauf 2020 und 2021 folgen. Für Österreich ist die Notifizierung mit dem Umstieg von Bürgerkarte und Handy-Signatur auf den neuen elektronischen Identitätsnachweis „E-ID" geplant, sodass Bürgerinnen und Bürger diesen ab 2021 zunehmend in Anwendungen in anderen EU-Staaten verwenden werden können, ab 2022 in öffentlichen Anwendungen aus den Anerkennungsverpflichtungen einen Anspruch darauf haben.

A-SIT ist zu eIDAS akkreditierte Konformitätsbewertungsstelle und kann so qualifizierte Vertrauensdiensteanbieter hinsichtlich der Einhaltung der

Vorgaben prüfen, sowie zertifiziert als Bestätigungsstelle qualifizierte Signatur- und Siegelerstellungseinheiten. A-SIT ist darüber hinaus in der internationalen Abstimmung eingebunden, indem es zusammen mit dem Bundesministerium für Digitalisierung und Wirtschaftsstandort Österreich in eIDAS Expertengruppen vertritt. Auch in Forschungsaktivitäten bringt A-SIT sich über die Beteiligung an EU Projekten zu eIDAS aktiv ein.

DI Herbert Leitold

Generalsekretär A-SIT

> *Der Themenbereich rund um E-Government, elektronische Signatur und elektronische Identität wurde von meinem Vorgänger als Institutsvorstand des IAIK, Prof. Reinhard Posch, mit viel Einsatz aufgebaut."*
>
> *Univ.-Prof. Dr. Stefan Mangard*

ID Austria

Digitale Ausweise und persönliche Daten

Der elektronische Identitätsnachweis (ID Austria) ist eine Weiterentwicklung der Handysignatur und bietet große Vorteile für BürgerInnen und Verwaltung sowie Potenziale für die Wirtschaft. Mit der ID Austria stehen künftig den BürgerInnen ihre Ausweise und persönlichen Daten erstmalig auch digital zur Verfügung. Die Hoheit über die eigenen Daten verbleibt dabei immer bei den BürgerInnen. Die BürgerInnen entscheiden selbst, welche personenbezogenen Daten an andere digital weitergegeben werden.

Für alle aktiven Handy-Signaturen erfolgt die Umstellung auf die ID Austria im bisherigen Nutzungsumfang. Für die Nutzung der neuen Funktionalitäten ist eine einmalige behördliche Registrierung erforderlich.

Die Registrierung kann für österreichische StaatsbürgerInnen von Amts wegen im Rahmen der Beantragung eines Reisepasses oder Personalausweises oder auf Verlangen bei einer Passbehörde erfolgen. Für Fremde ist die Landespolizeidirektion zuständig. Es findet immer eine umfassende behördliche Prüfung der Identität statt. Die staatlich gesicherte ID Austria ermöglicht BürgerInnen somit Rechtssicherheit in digitalen Prozessen sowie Schutz vor Identitätsdiebstahl und Cyberkriminalität.

Um die ID Austria zu nutzen, muss der Bürger das 14. Lebensjahr vollendet haben und über ein Smartphone mit der App „Digitales Amt“ inkl. einer Touch-ID (Fingerabdruck) bzw. einer aktivierten Gesichtserkennung (Face-ID) verfügen.

Die Login-Funktionalität – und somit der elektronische Nachweis der Identität des Anwenders – kann für österreichische Onlineverfahren und -anwendungen verwendet werden. Es ist angedacht, diese Funktion auch in elektronischen Anwendungen anderer EU-Länder nutzen zu können, allerdings werden die geplanten Ausweisfunktionalitäten vorerst nur in Österreich nutzbar sein.

„Die staatlich gesicherte ID Austria ermöglicht BürgerInnen Rechtssicherheit in digitalen Prozessen sowie Schutz vor Identitätsdiebstahl und Cyberkriminalität.“

A-SIT TIPP

Sollten Sie Verdacht oder konkrete Hinweise auf Internetkriminalität haben, können Sie sich an die Meldestelle des BMI wenden:

against-cybercrime@bmi.gv.at

Bei Straftaten durch konkrete Personen können Sie diese in jeder Polizeidienststelle anzeigen

Die ID Austria ist ab dem Tag des Ab-

„Die BürgerInnen entscheiden selbst, welche personenbezogenen Daten an andere digital weitergegeben werden."

schlusses der Registrierung fünf Jahre gültig und kann von österreichischen StaatsbürgerInnen im Self-Service um weitere fünf Jahre verlängert werden. Das geplante System stellt ein Angebot an die BürgerInnen sowie an die Wirtschaft dar. Datensicherheit ist ein Recht der BürgerInnen und eine Pflicht der Verwaltung. Durch die verstärkte Nutzung von digitalen Identitäten im Alltag wird auch das Angebot digitaler Leistungen in der Verwaltung zunehmen. Darüber hinaus werden der Wirtschaft Chancen eröffnet, praktische Services, neue Geschäftsideen und sichere Prozesse für den Wirtschaftsstandort auf Basis von staatlich gesicherten Identitäten zu entwickeln. Digitale Geschäftsabschlüsse werden schneller, der Austausch mit den Behörden wird einfacher.

Damit wird jedem Benutzer ermöglicht, die eigenen Verwaltungs- und Geschäftsprozesse sicher auf einer zukunftsgerichteten digitalen Basisinfrastruktur zu erledigen und somit die Digitalisierung in Österreich konstruktiv voranzutreiben.

Bundesministerium für Inneres

Abteilung IV/6
IKT-Strategie und IKT-Governance

ID Austria
Digitaler Identitätsnachweis

ELEKTRONISCHER AUSWEIS FÜR DIE NUTZUNG ELEKTRONISCHER SERVICES IM INTERNET

Die Bürgerkarte wurde 2004 als elektronischer Ausweis der österreichischen Bevölkerung für die Nutzung elektronischer Services im Internet eingeführt. Für eine wesentliche Verbesserung der Benutzerfreundlichkeit sorgte die Einführung der Handy-Signatur Ende 2009, die die Bürgerkartenfunktion auf einem Mobiltelefon ermöglichte. Das Konzept „Bürgerkarte/Handy-Signatur" wird 2021 zu einem digitalen Identitätsnachweis „ID Austria" weiterentwickelt.

Mit der ID Austria soll die Verwendung der elektronischen Identität erleichtert und dessen rechtliche Anerkennung, gemäß der EU-Verordnung zur „elektronischen Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" (eIDAS Verordnung), auch in anderen europäischen Ländern herbeigeführt werden. Auch die Nutzungsmöglichkeiten von Bürgerkarte/Handy-Signatur werden mit der ID Austria erweitert, indem künftig auch weitere Personenmerkmale (Attribute) aus behördlichen Registern, an dritte Stellen (z.B. elektronische Dienstanbieter) übermittelt werden können.

Die Entscheidung, ob Daten an Dritte übermittelt werden dürfen, obliegt dem/der betroffenen Bürger/Bürgerin.

Einen wesentlichen Vorteil der ID Austria stellt der verbesserte Schutz der Privatsphäre personenbezogener Daten dar. Mit der ID Austria besteht für private Services die Möglichkeit, das Geburtsdatum einer Bürgerin/eines Bürgers, ohne die Offenlegung des Namens, nachzuweisen. In bestimmten Fällen könnte auch nur eine Bestätigung der Volljährigkeit genügen. Jede Transaktion wird protokolliert und ist nur der jeweiligen Person und dem Betreiber des Service zur Nachvollziehung zugänglich. Damit können BürgerInnen und Bürger jederzeit überprüfen, an wen, zu welchem Zeitpunkt, welche Personenmerkmale übermittelt wurden.

„Die Entscheidung, ob Daten an Dritte übermittelt werden dürfen, obliegt dem/der betroffenen Bürger/Bürgerin."

Die Einführung der ID Austria wird auch eine Änderung des Registrierungsprozesses mit sich bringen. Die Registrie-

„Die Gültigkeitsdauer der ID Austria beträgt 5 Jahre und kann nach Ablauf über ein Self-Service von Bürgerinnen und Bürgern verlängert werden."

rung einer ID Austria für Bürgerinnen und Bürger wird künftig ausschließlich bei Passbehörden, Landespolizeidirektionen und weiteren noch festzulegenden Behörden möglich sein. Personen, die einen Reisepass beantragen oder verlängern, erhalten automatisch eine ID Austria, wenn sie auf diesen nicht ausdrücklich verzichten. Die Gültigkeitsdauer der ID Austria beträgt 5 Jahre und kann nach Ablauf über ein Self-Service von Bürgerinnen und Bürgern verlängert werden. Bestehende Handy-Signaturen können von der Bürgerin bzw. dem Bürger in eine ID Austria mit dem Funktionsumfang der bisherigen Handy-Signatur übergeführt und bis zu ihrem Ablauf weiterhin genutzt werden.

Anschließend muss jedoch eine „vollumfängliche" ID Austria bei einer zur Ausstellung ermächtigten Behörde registriert werden.

Dr. Arne Tauber

Head of eGovernment
Innovation Center (EGIZ)

Tricks und Täuschungsmanöver mobiler Angreifer

Trotz steigender Beliebtheit bei Angreifern ist Android ein vergleichsweise sicheres System. Dennoch: Selbst perfekt funktionierende Apps, deren Daten komplett isoliert sind, können unbemerkt gekapert werden. Sogenannte „Overlay-Angriffe" überlagern unauffällig legitime Anwendungen und gelangen so an gefährliche Berechtigungen und sensible Daten, z.B. von Banking-Apps, Messengern oder Browsern.

Gut getarnt: Welches Fenster ist von welcher App?

Für einen erfolgreichen Overlay-Angriff muss die bösartige App laufende Tasks erkennen. Ein Weg ist die TaskAffinity: Der TaskManager führt den Schadcode aus, wenn die legitime App gestartet wird, und verschiebt das eigentliche Fenster in den Hintergrund – Daten werden unbemerkt in die Schadsoftware eingegeben. Diese als „StrandHogg" bekannte Schwachstelle wird aktiv „in the Wild" ausgenutzt und betrifft alle Android-Versionen.

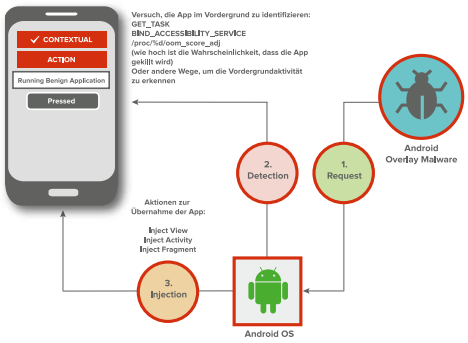
Andere Angriffe schleusen einzelne Objekte in die Vordergrundaktivität ein oder laden Content nach. Werden die Overlays als Systembenachrichtigung definiert, können sie nicht weggeklickt werden. Mit dieser Technik sperren auch Ransomware-Attacken die Geräte.

Gut gemacht: Gezielte Angriffe auf Bank-Apps

All diese Szenarien setzen voraus, dass sich am Zielgerät bereits Schadsoftware befindet. Angreifer senden dazu z.B. eine SMS an die User bestimmter Bank-Apps und schildern ein dringendes Szenario wie ein notwendiges Sicherheits-Update. Etwas Druck, etwa durch die Drohung, das Konto würde andernfalls gesperrt, steigert die Downloadquote. Dann verlangt die gefälschte Bank-App tiefgreifende Berechtigungen wie das Mitloggen der Tastatur oder Ändern der Standard-SMS-App – immer getarnt als Systemdialog oder andere Anwendung. Und schon kann die Schadsoftware unabhängig operieren, Passwörter mittracken und heimlich an den Zielserver schicken.

Neben einem professionellen Malwarescanner schützen Sie sich am besten mit einer gesunden Portion Skepsis und dem Prinzip mehrerer Kanäle: Fragen Sie beim leisesten Verdacht auf einem anderen Weg nach!

MSc Tibor Éliás
Android Malware Analyst
IKARUS Security Software GmbH



A-SIT TIPP

Wenn Unternehmen Opfer einer Cyberattacke, oder eines Cybercrime-Angriffs bzw. von Ransomware oder Verschlüsselungstrojanern wurden, dann bietet die Cyber-Security-Hotline der WKO (für Mitglieder kostenlos) rund um die Uhr telefonische Erstinformation und Notfallhilfe unter:

Tel: 0800 888 133

Zur Verbesserung der Sicherheit bedarf es gerade im Umfeld mobiler Banking-Apps einer ständigen Technologiebeobachtung, damit innovative Lösungen schnell integrierbar sind bzw., um in geeigneter Form auf Probleme reagieren zu können. Vor allem die Weiterentwicklung bei hardware-basierten Sicherheitselementen sowie damit verbundene Software-Komponenten sind hier sehr relevant und müssen adäquat berücksichtigt werden"

Dr. Peter Teufi, CEO A-SIT Plus GmbH

Schadsoftware für mobile Plattformen

ZUVERLÄSSIGE ERKENNUNG MIT PROGRAMMANALYSE

Schadprogramme gibt es seit Jahrzenten, aber die Taktiken der Angreifer entwickeln sich ständig weiter, wenn es darum geht neue Sicherheitslücken auszunützen, um sich weiterzuverbreiten und neue Geschäftsmodelle zu finden. Zusätzlich zu Malware „von der Stange" wird zielgerichtete Malware zu Spionagezwecken oder für Angriffe auf kritische Infrastruktur, wie im Fall von Stuxnet, verwendet.

Projekte wie Anubis bzw. die Android-Variante Andrubis verwenden automatische Programmanalyse, um das Verhalten von Software in einer kontrollierten Umgebung zu beobachten. In Kombination mit Machine Learning können wir auch Entscheidungen über die „Schädlichkeit" eines Programmes treffen. Teilweise braucht es dafür aber einen Kontext: Cryptominer z.B. werden teilweise bewusst eingesetzt, sind aber im Unternehmensumfeld unerwünscht. Mit unsere Studie MineSweeper haben wir u.a. gezeigt, dass kompromittierte Webseiten genutzt werden, um mit der Rechenleistung der Besucher Geld zu machen und wie man dieses Verhalten zuverlässig erkennen kann. Neben üblicher Schadsoftware operieren auch legitime Apps oft im Graubereich des Datenschutzes: Teilweise ohne das Wissen des App-Entwicklers sammeln vor allem Drittservices vermehrt Benutzerdaten. Auch in diesem Bereich setzen wir auf Programmanalyse, um die Datensammlung und potentielle Sicherheitslücken in der Datenübertragung sichtbar zu machen.

Wir arbeiten daran unsere Analysetechniken weiterzuentwickeln und plattform-unabhängiger zu machen: Einerseits wird iOS zwar oft als sicherer betrachtet, wissenschaftliche Studien gibt es dazu aber kaum. Andererseits werden Verbrauchergeräte immer intelligenter, sind im Rahmen von Smart Homes und Büros mit anderen Geräten verbunden und in der Regel dauerhaft online. Gesteuert werden diese IoT Geräte überwiegend über Apps und Assistenten. In einem vom WWTF geförderten Projekt untersuchen wir Steuerungsapps und Kommunikationsprotokolle, um Rückschlüsse auf potenzielle Sicherheitslücken zu ziehen.

Prof. Dr.in Martina Lindorfer

Assistant Professor
TU Wien, Fakultät für Informatik
Fachbereich Security & Privacy
Secure Systems Lab

A-SIT TIPP

Scheuen Sie bei Abzocke und Betrugsversuchen nicht den Kontakt mit der zuständigen Meldestelle.

Die Watchlist Internet listet auf Ihrer Webseite zahlreiche Artikel über verschiedenste Betrugsversuche, wie etwa Fake-Shops, Pishing, gefälschte Rechnungen und Abo-Fallen.

Weiters führt sie eine Liste betrügerischer Online-Shops. Falls Sie einen Betrugsversuch entdeckt haben oder einen Verdacht haben, melden Sie diesen über das Melde-Formular:

www.watchlist-internet.at

A-SIT TIPP

Wenn Sie betroffen sind oder einen Schaden erlitten haben bzw. erleiden werden, wenden Sie sich an die Internet Ombudsstelle.

Diese Meldestelle bietet Hilfe bei der Streitschlichtung sowie kostenlose Online-Beratung rund um „Einkaufen im Internet“:

www.ombudsstelle.at

Andreas Minnich
Abgeordneter zum Nationalrat

Datensicherheit für die Menschen

Wenn wir über Digitalisierung als Zauberwort für die Zukunft sprechen, müssen wir aber auch über Sicherheit nachdenken. Der Datenschutz ist ein zentrales Thema und zwar sowohl für Bund, Land, Gemeinden sowie jeden Einzelnen.

Wenn Sicherheit und Diskretion an oberster Stelle stehen, dann sind das Vertrauen und die Expertise bei A-SIT der logische nächste Schritt zu mehr Cyber-Security.

TOPIC 3

Cybercrime, Schadsoftware & Erste Hilfe

Internetkriminalität

Die globale Vernetzung und die zunehmende Technisierung sowie Digitalisierung eröffnen Kriminellen ständig neue Möglichkeiten, um ihre Opfer zu schädigen. Die Anzahl der Cybercrime-Delikte steigt daher kontinuierlich: 28.439 Anzeigen wurden 2019 erstattet, 44,9 Prozent mehr als im Vorjahr.

„Bei Cyber-Crime-Delikten konnten wir die Aufklärungsquote auf 35,8 Prozent steigern."

Trotz des großen Anstiegs konnte die Aufklärungsquote auf 35,8 Prozent gesteigert werden. Durch die Verlagerung der klassischen Welt in den digitalen Kontext treten vermehrt Massenphänomene, wie Massenerpressungs-E-Mails oder Ransomware auf. Die Polizei hat rasch auf diese Massen-E-Mails reagiert und eine eigene Arbeitsgemeinschaft gegründet.
Hinsichtlich des Phänomens der Ransomware konnten 2019 signifikante Veränderungen festgestellt werden: Waren es zunächst Einzelpersonen, die mit der Entschlüsselung ihrer Daten erpresst wurden, verlagerte sich das Opferprofil vermehrt Richtung kleine und mittlere Unternehmen. Zudem passten die Täter die Höhe der Erpressungssummen an den Umsatz und die Verschlüsselungsprozesse an die Backup-Strategien der Geschädigten an. Durch die technischen Anpassungen und Änderungen der Modus Operandi bleibt Ransomware eine der größten Gefahren, um einen Datenverlust zu erleiden.

Die Strategien zur Bekämpfung von Cybercrime erstellt in Österreich das Cybercrime Competence Center (C4) des Bundeskriminalamts. Das C4 ist nationale und internationale Koordinierungs-, Ermittlungs- und Meldestelle für Cybercrime und zudem für die elektronische Beweismittelsicherung und Auswertung zuständig. Darüber hinaus ist im C4 eine eigene Meldestelle eingerichtet, die nicht nur Verdachtsmeldungen rund um die Uhr entgegennimmt, sondern auch Auskunft erteilt. Sie ist unter against-cybercrime@bmi.gv.at erreichbar.

Erhard Friessnik

Bundeskriminalamt, Leiter des Cybercrime-Competence-Centers C4

MELDESTELLEN

RELEVANTE KONTAKTADRESSEN ZUR MELDUNG VERSCHIEDENER VORFÄLLE

Abzocke & Betrug

Scheuen Sie bei Abzocke und Betrugsversuchen nicht den Kontakt mit der zuständigen Meldestelle.

Die Watchlist Internet listet auf ihrer Webseite zahlreiche Artikel über verschiedenste Betrugsversuche, wie etwa Fake-Shops, Phishing, gefälschte Rechnungen und Abo-Fallen. Weiters führt sie eine Liste betrügerischer Online-Shops. Falls Sie einen Betrugsversuch entdeckt haben oder einen Verdacht haben, melden Sie diesen über das Melde-Formular: **www.watchlist-internet.at**

Wenn Sie betroffen sind oder einen Schaden erlitten haben bzw. erleiden werden, wenden Sie sich an den Internet Ombudsstelle. Diese Meldestelle bietet Hilfe bei der Streitschlichtung sowie kostenlose Online-Beratung rund um „Einkaufen im Internet“: **www.ombudsstelle.at**

Internetkriminalität

Sollten Sie Verdacht oder konkrete Hinweise auf Internetkriminalität haben, können Sie sich an die Meldestelle des BMI wenden: **against-cybercrime@bmi.gv.at**

Bei Straftaten durch konkrete Personen können Sie diese in jeder Polizeidienststelle anzeigen.

Kinderpornografie & Kindersextourismus

Sollten Sie im Internet kinderpornografisches Material oder Angebote von Sextourismus mit Kindern entdecken, können Sie den Fund dem BMI melden oder aber auch Anzeige in jeder Polizeidienststelle erstatten: **meldestelle@interpol.at**

Nationalsozialismus & radikaler Islamismus

Sollten Sie auf neonazistische, rassistische oder antisemitische Inhalte stoßen, können Sie den Fund an die Meldestelle des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT) melden oder aber auch Anzeige in jeder Polizeidienststelle erstatten: **ns-meldestelle@bvt.gv.at**

Falls Sie auf extremistische und radikale Videos, die einen Bezug zu Österreich haben, stoßen, dann können Sie dies an die Meldestelle des BVT weiterleiten: **stopextremists@bmi.gv.at**

i

Weitere Details zu Meldestellen sind auf dem Informationssicherheitsportal abrufbar unter:

www.onlinesicherheit.gv.at

Digitale Transformation aus der Sicht des Technikrechts

Das Voranschreiten technologischer Entwicklungen und der damit verbundene Einfluss auf die Gesellschaft allgemein sowie auf die Rechtsordnung im Speziellen ist kein Novum des vergangenen Jahrzehnts, nicht einmal des vergangenen Jahrhunderts. Die Kommunikation gibt dafür ein gutes Beispiel ab: Im Jahr 1837 stellte Samuel Morse den Prototyp eines ersten elektrischen Telegrafen vor, die Einführung von Telegrafenanlagen in Österreich erfolgte im Jahr 1846. Das Telefon, Radio sowie Fernsehen folgten. Die flächendeckende Einführung des Internets in Österreich erfolgte Anfang der 1990er-Jahre. Diese Entwicklungen warfen stets Rechtsfragen auf und führten zu – teils erheblichen – Rechtsänderungen. Vorstellungen, wie die vom Internet als „rechtsfreiem Raum", konnten der rechtlichen Realität nicht Stand halten.

Die Nutzung des Internets als Massenmedium hat wesentlich zugenommen. Gleichzeitig fanden auch bahnbrechende Entwicklungen auf unterschiedlichsten Gebieten statt, auf die das geltende Recht teils nicht einfach ersichtliche, nur unzureichende, ungeeignete oder gar keine Antworten gibt. Der Gesetzgeber sah sich in der Vergangenheit – und sieht sich nach wie vor – mit dem Problem konfrontiert, dass die von ihm erlassenen Steuerungs- oder Regulierungsmaßnahmen bereits nach kurzer Zeit wieder inaktuell werden. Ein besonders eindrucksvolles Beispiel dafür ist die Datenschutzgrundverordnung (DSGVO), die zwar bewusst technologieneutral formuliert wurde und dennoch Aspekte der künstlichen Intelligenz nur am Rande (als „automatisierte Entscheidungen") berücksichtigt (zB Art 22 DSGVO). Die Europäische Union bemüht sich bereits seit langem um eine Vereinheitlichung der Rechtslandschaft, insbesondere auch mit Blick auf den Schutz kritischer Infrastruktur. So wurde als Reaktion auf den zunehmenden Anstieg von Sicherheitsverletzungen schon im Jahr 2004 die Europäische Agentur für Cybersicherheit (ENISA) errichtet, die Richtlinie zur Netz- und Informationssystemsicherheit (NIS-RL) wurde im Jahr 2013 erlassen und in Österreich

> „Technische Entwicklungen warfen stets Rechtsfragen auf und führten zu – teils erheblichen – Rechtsänderungen."

(1) Leitner, IT-Sicherheitsrecht, in Felten et al (Hg), Digitale Transformation im Wirtschafts- und Steuerrecht (2019) Rz 52.
(2) Leitner, IT-Sicherheitsrecht, in Felten et al (Hg), Digitale Transformation im Wirtschafts- und Steuerrecht (2019) Rz 60.
(3) AB 799 BlgNR 27. GP 1.
(4) Der Standard (Hg), Impfstoffdaten bei Hackerangriff auf EU-Gesundheitsbehörde abgegriffen, https://bit.ly/3t02hhf (Stand 10.12.2020).
(5) Der Standard (Hg), Hacker leaken gestohlene Daten zu Pfizers Corona-Impfstoff, https://bit.ly/3prtCXu (Stand 13.01.2021).
(6) Europol (Hg), Internet Organized Crime Threat Assessment 2020, 6, https://bit.ly/2M7wpXy (abgefragt 14.01.2021).

im Jahr 2018 als Netz- und Informationssystemsicherheitsgesetz (NISG) umgesetzt.[1] Sowohl Anbieter digitaler Dienste gem § 3 Z 12 NISG (darunter insb. auch Cloud-Computing-Dienste), aber auch durch den Mitgliedstaat bestimmte Betreiber wesentlicher Dienste aus bestimmten Sektoren (zB Energie, Bankwesen, digitale Infrastruktur wie etwa DNS-Diensteanbieter) gem. § 2 NISG sind zu umfassenden technischen und organisatorischen Maßnahmen verpflichtet, um externe Angriffe abzuwehren.[2] Zum Stichtag 7. Februar 2020 wurden bislang 37 Betreiber solcher wesentlichen Dienste identifiziert.[3] Die Notwendigkeit der gesetzlichen Verankerung von Schutzstandards zeigt sich besonders in spektakulären Attacken auf kritische Infrastruktur in der Vergangenheit, wie etwa der jüngste Einbruch in das Netzwerk der Europäischen Arzneimittelbehörde (EMA). Im Zuge dieses Angriffs wurden Daten im Zusammenhang mit der Zulassung von Impfstoffen gegen das COVID-19-Virus gestohlen[4] und veröffentlicht.[5] Die COVID-19-Pandemie führte – aufgrund der gesellschaftlichen Einschränkungen während der Lockdowns – zu einem massiven Anstieg an Cyberkriminalität, wobei Ransomware- und DDos-Attacken, sowie Angriffe mittels Social Engineering besonders hervorzuheben sind.[6]

Damit zeigt sich einmal mehr die Notwendigkeit der Schaffung klarer gesetzlicher Grundlagen, um die „Grundfesten der Digitalisierung" wie etwa kritische Infrastruktur, aber auch wesentliche digitale Dienste vor Angriffen zu schützen, und deren Betreiber zu umfassenden Schutzmaßnahmen zu verpflichten. Breites Vertrauen in digitale Technologien ist eine wesentliche Grundbedingung für die digitale Transformation vieler Bereiche. Das Recht als zentrales Steuerungsinstrument des Staates muss dazu beitragen, Vertrauen zu schaffen. Die bereits dafür zur Verfügung stehenden Regelwerke (insb die DSGVO, das NISG, aber auch die eIDAS-Verordnung) stellen durchaus taugliche, wenngleich nicht ideale Grundlagen dar. Aufgrund der rasanten technologischen Entwicklung sind technologieneutrale Formulierungen essentiell, um deren längerfristige Anwendbarkeit zu gewährleisten. Die Festlegung von Schutzstandards sollte zudem aus Gründen der Vereinheitlichung vornehmlich auf europäischer Ebene erfolgen. Hinzu muss die Möglichkeit treten, rechtliche Rahmenbedingungen in Reallaboren oder Sandboxes zu erproben und weiterzuentwickeln. Rechtswissenschaftliche Forschung, wie sie das Linz Institute of Technology (LIT) Law Lab leistet, muss im interdisziplinären Zusammenspiel mit den technischen Wissenschaften und etwa auch den Sozialwissenschaften ein belastbares wissenschaftliches Fundament für die notwendigen Rechtsentwicklungen leisten.

Univ.-Prof. Dr. Michael Mayrhofer
Dekan der Rechtswissenschaftlichen Fakultät, Leiter des LIT Law Lab, JKU Linz

Univ.-Ass. Rechtsanwalt Mag. Philipp Leitner
Wissenschaftlicher Mitarbeiter Linz Institute of Technology (LIT) Law Lab, JKU Linz

CYBERBELT
Fragen & Antworten

DI Dr.tech Wolfgang Prentner

CEO, IT-Ziviltechniker, Informatiker
ZTP.digital ZT-GmbH, Prüfstelle für Digitale Sicherheit

Was sind die häufigsten Bedrohungsszenarien für Unternehmen?

Cyber-Angriffe in Form von Malware sind weltweit verbreitet. Die Malware „Emotet" beispielsweise verbreitet sich häufig über Spam- bzw. Phishing-Mails. Dabei werden Fake-E-Mails – die angeblich von Großunternehmen stammen – massenweise mit schadhaften Anhängen (z.B. Dokumente, wie eine Rechnung mit korrupten Makros) versendet. Nachdem sich die Schadsoftware erfolgreich eingeschleust hat, verbreitet sie sich über das lokale Netz. Mit Ransomware kann man sich über E-Mails infizieren, aber auch über Schwachstellen im Browser, Betriebssystem oder in Programmen – dies kann zu fatalen Folgen führen (Beispiel: Ausfälle in der Produktion).
Durch Identitätsdiebstahl gelingt es Cyber-Kriminellen mithilfe von Social-Engineering-Methoden, Schadsoftware oder durch Daten-Leaks an personenbezogene Daten heranzukommen, um sie für kriminelle Zwecke zu verwenden.

Wie kann man sich schützen?

Cyber-Angriffe haben viele Gesichter, demnach gibt es unterschiedliche Methoden um sich vor dieser noch unterschätzten Bedrohung zu schützen.

Nach dem Motto „Vorsicht ist besser als Nachsicht" empfehle ich:

- Eine wirkungsvolle Maßnahme ist es, ein ganzheitliches Informationssicherheitsmanagementsystem umzusetzen, um die Basis-Anforderungen festzulegen.
- Schulen Sie Ihre Mitarbeiter ein! – Mithilfe der Security-Awareness-Schulung stärken Sie die digitale Eigenverantwortung.
- Backups
- Antivirensoftware
- Patchmanagement
- Netzwerksegmentierung
- Firewalling
- E-Mail-Filter
- Web-Content-Filter
- u.v.m.

Was kann man tun – wenn die Bedrohung bereits akut ist?

Ist der Bedarfsfall eingetreten, ist schnelles Handeln wesentlich. Am besten ist es, wenn Sie einen IT-Sicherheits-Experten konsultieren – wie z.B. ZTP.digital – Die Prüfstelle für Digitale Sicherheit. Bei Notfällen handeln wir sofort um den Schaden möglichst gering zu halten bzw. zu beseitigen.
Im Falle von Ransomware empfehle ich hier ganz klar: Ignorieren bzw. die Fake-Rechnung nicht bezahlen. Eine einfache Möglichkeit um die Ausbreitung der Schadsoftware innerhalb des lokalen Netzes zu verhindern, ist es eine Spezial-Software einzusetzen oder im Notfall das System herunterzufahren.

Was ist der CyberBELT-Schutz – den Sie anbieten?

Mit Hilfe des CyberBELTs werden Ihnen bis zu 52 Schwachstellenberichte pro Jahr (ein Bericht/Woche) über den Gesundheitszustand Ihrer Systeme von ZTP.digital geliefert. Damit erkennen Sie frühzeitig Gefahren für Ihr Unternehmen und setzen so die richtigen Schutzmaßnahmen auf Basis unserer Prüfberichte um.

Mit dem CyberBELT garantiert ZTP.digital Ihnen Cyber-Sicherheit und Datenschutz mit einem staatlich anerkannten Cyber-Sicherheitszertifikat auf Basis der aktuellen Gesetze, Standards und Richtlinien.

„Ist der Bedarfsfall eingetreten, ist schnelles Handeln wesentlich."

Infos zum CyberBELT:

CyberBELT	Ihr Internet-Sicherheitsgurt
Dienstleistungen	Sicherheits-Audits
	Pentesting
	Social Hacking – Red Team Operations
	Code Analysen
CyberBELT-Sicherheits-formel:	sammeln + prüfen + überwachen = Zertifikat "Cyber-Sicherheit"
Kontakt	https://cyberbelt.net info@cyberbelt.net

Eine Dienstleistung der ZTP.digital ZT-GmbH, Prüfstelle für Digitale Sicherheit, staatlich befugt und beeidet.
Austria I Europe I www.ztp.digital

CYBERBELT

Ihr Internet-Sicherheitsgurt

Was ist der CyberBELT?
Und was passiert, wenn geheime Daten wie Patienteninformationen, Bank- oder Kundendaten, Bilanzen, Passwörter oder elektronische Urkunden von Fremden gestohlen, veröffentlicht oder missbraucht werden?

Diese Szenarien sind heute bereits Realität. Doch wie kann das vermieden werden ohne dafür auch noch zu haften? Ganz einfach! Mit dem CyberBELT, dem Internet-Sicherheitsgurt von ZTP. Der CyberBELT garantiert Ihnen Cyber-Sicherheit und Datenschutz mit einem staatlich anerkannten Zertifikat auf Basis der aktuellen Gesetze, Standards und Richtlinien. Durch mächtige Scan-Werkzeuge, sammeln von Daten und gezielten Angriffen werden Ihre Websysteme geprüft und auf Basis des aktuellen Standes der Technik überwacht. Monatlich oder wöchentlich, je nach Risikoklassifizierung, erhalten Sie einen persönlichen Gesamtbericht zum Gesundheitszustand Ihrer Systeme mit kritischen, hohen und mittleren Schwachstellen, welche umgehend von Ihnen oder Ihrem Dienstleister behoben werden müssen.
Durch die Zertifizierung der von uns geprüften Systeme haftet ZTP für die Sicherheit Ihrer Systeme, sollten Sicherheitslücken durch Prüfungsfehler unsererseits verursacht worden sein. Die kontinuierliche Überwachung von außen sowie die regelmäßige Auditierung der IT-Systeme vor Ort einmalig, für 12 oder 24 Monate bietet einen erhöhten Schutz vor fremdem Zugriff und liefert Informationen zum Aufbau einer Abwehrstrategie um Angriffe erfolgreich abzuwehren.

„Der CyberBELT garantiert Ihnen Cyber-Sicherheit und Datenschutz mit einem staatlich anerkannten Zertifikat."

Erhöhen Sie Ihre Cyber-Sicherheit und verhindern Sie Vertrauensverlust, hohe Strafen und Imageschäden durch Objektivität und fachliche Kompetenz durch ihr staatlich beeidetes Sicherheitszertifikat und einer Beilage zur Jahresabschlussprüfung, welche immer öfters auch technische Sicherheits- und Compliance-Bestätigungen verlangen.

CyberBELT – Ihr Internet-Sicherheitsgurt für mehr Sicherheit und Vertrauen in die Informationstechnologie.

ZTP – Ihre Prüfstelle für Digitale Sicherheit

https://cyberbelt.net
Millennium Tower,
Handelskai 94-96, 1200 Wien

DI Dr.tech Wolfgang Prentner
CEO, IT-Ziviltechniker, Informatiker
ZTP.digital ZT-GmbH

CYBERBELT©

IHR INTERNET-SICHERHEITSGURT

Sicherheits-Audit

Pentesting

Social Hacking

Red Team Operations

Code Analysen

mit **Zertifikat**

cyberbelt.net

ZTP

Prüfstelle für Digitale Sicherheit

Der ungebetene Gast im Netzwerk

Wirtschaftsspionage als Problem

Das war sie also – diese Mail mit dem angeblich angehängten Protokoll zur Durchsicht das sich leider nicht öffnen ließ. Dabei klang der Text des Mails sehr vertraut und bezog sich auf zuletzt entwickelte Kontakte zu einem neuen Geschäftspartner. Die Auswirkungen dieser Mail waren leider fatal! Automatisch installierte sich ein kleines Softwaremodul und prüfte die Internetverbindung durch einen „Ping" zu einer viel frequentierten Website. Danach lud der Neuankömmling neue Softwaremodule von einem Command&Control (C&C) Server nach, erstellte einen Cryptocontainer und begann, das Netzwerk zu erforschen und sich in ebendiesem tief zu verankern. Ziel waren technische Informationen, Verbindungsknoten nach außen sowie Konfigurationsdaten, Informationen zu Systemlücken und Passwörter. Nachdem diese Daten in den Cryptocontainer geladen waren, wurden verdächtige Daten gelöscht und ein weiteres Modul zur Analyse von Verbindungsinformation und Feststellung bestmöglicher Sendezeiten nachgeladen. Anschließend erfolgte die Weiterleitung der gesammelten Informationen an den C&C Server und ein weiteres Modul begann die Verbindungsinformationen zu nutzen und sich auf weitere Systeme auszubreiten. Leider erkannten die unternehmenseigenen Sicherheitssysteme (wie z.B. Firewalls oder Intrusion Detection Systeme) diesen komplexen Angriff nicht und erst durch einen externen Hinweis wurde der Verdacht untersucht,

> „So lesen sich vermehrt Sachverhalte die für die betroffenen Einrichtungen zu einem elementaren Problem wurden."

Angriff erkannt und durch Maßnahmen eingedämmt und schließlich bereinigt.

So lesen sich vermehrt Sachverhalte, die für die betroffenen Einrichtungen zu einem elementaren Problem wurden. Das Internet, die globale Vernetzung, Sicherheitslücken in Softwareprodukten, ständig neue Updates sowie der Einsatz neuer Technologien bergen Risiken, die oft nur mangelhaft in den Risikoanalysen und –strategien abgebildet sind. Dies ist eine immense Gefahr für Geschäfts- und Betriebsgeheimnisse und eine Herausforderung für die Risikoanalysen von Unternehmen, kritischen Infrastrukturen aber auch Behörden. Oft verlässt man sich dabei auf die Unternehmens IT, aber diese ist möglicherweise kein Garant für Cybersicherheit.

Stellt sich natürlich die Frage, ob Unternehmen und Institutionen ausrei-

chend auf solche Gefahren vorbereitet sind. Sind Geheimschutz, Cybersicherheit und Datenschutz Teil der institutionellen Risikolandschaft? Bestehen Prozesse, die den Umgang mit diesen Risiken definieren? Gibt es interne CS Expertise? Gibt es Kontakte zu externen CS Experten oder jenen Behörden, die sich mit diesen Themen befassen? Hat das Unternehmen an die Möglichkeit einer CS Versicherung gedacht und umfasst diese das gesamte CS Risikopotenzial? Sind die Mitarbeiter mit dem Thema CS vertraut? Der informierte User ist oft ein Schlüssel zum Erkennen und Verhindern von Angriffen! Existiert eine Kommunikationsstrategie für solche Fälle und ist sie vor allem auf Kunden, Partner, Behörden aber auch auf die Öffentlichkeit ausgerichtet. So vorbereitet lässt sich ein komplexer Angriff sicherlich leichter handhaben. Dennoch bedeutet er eine Herausforderung für das Image des Unternehmens oder der Institution, Kosten und möglicherweise auch lange Verfahren mit geringen Aussichten auf Erfolg.

> *Vor allem in der Wirtschaftsspionage basieren Angriffe oft auch auf Zero-Day-Exploits. Da ein 100-prozentiger Schutz gegen solche Angriffe kaum möglich ist, müssen neben herkömmlichen Schutzmaßnahmen rechtzeitig auch Vorkehrungen für den Fall eines erfolgreichen Angriffs getroffen werden."*
>
> *Dr. Thomas Zefferer,*
> *Senior IT-Security Expert A-SIT Plus GmbH*

Zu den Aufgaben des BVT gehören u.a. der Schutz verfassungsmäßiger Einrichtungen und kritischer Infrastrukturen sowie die Abwehr von Wirtschaftsspionage. Gerade die schwierige Zuordnung von Cyber- oder Spionageangriffen und die geringen Aussichten, der Täter habhaft zu werden führen dazu, dass das BVT Vorbeugung und Prävention oberste Priorität einräumt. Dazu zählen jedenfalls die Fähigkeiten, Angriffe zu erkennen und sie abzuwehren oder einzudämmen. Geheimschutz und Cybersicherheit brauchen einen wichtigen Stellenwert in der Risikolandschaft des Unternehmens und sollten in entsprechende Prozesse zur Abarbeitung von solchen Vorfällen münden. Dabei können Kontakte zu externen Experten in Wirtschaft und Behörden von enormer Wichtigkeit sein.

Externe Hilfestellung hat aber nur dann Aussicht auf Erfolg, wenn das betroffene Unternehmen auch bereit ist, vorbehaltslos jene Information zu teilen, die zur Abwehr des Angriffs notwendig ist und schließlich den Schlussfolgerungen aus dem Angriff und den Empfehlungen der Experten auch zu folgen.

Mag. Peter Gridling
Direktor BVT

Meltdown, Spectre & Co. Mikroarchitekturangriffe

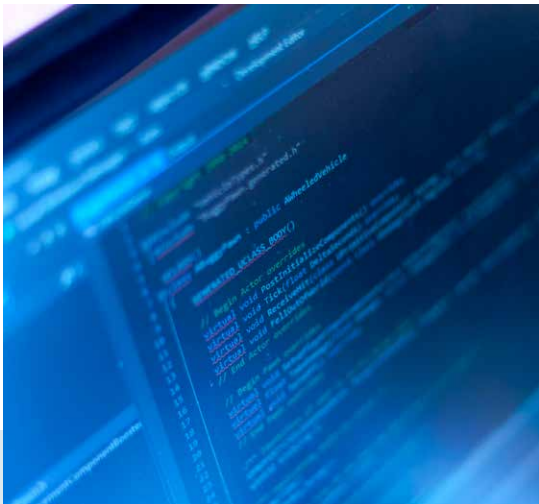
FEHLERHAFTE HARDWARE LÄSST DATEN DURCHSICKERN

Um den Bedarf an schnelleren und effizienteren Computern trotzdem zu decken, wurden neben Taktraten und Strukturgrößen vor allem methodische Optimierungen eingeführt, von denen zwei besonders signifikant sind. Erstens „Caching“, eine Technik, die dem Prozessor eine Art Kurzzeitgedächtnis gibt, aus dem kürzlich verarbeitete Daten oder Ergebnisse schnell wieder aufgerufen werden können. Zweitens „Out-of-Order Execution“, eine Technik die dem Prozessor erlaubt, Arbeitsschritte

„Diese natürlichen Optimierungen führen aber auch zu Sicherheitsproblemen.“

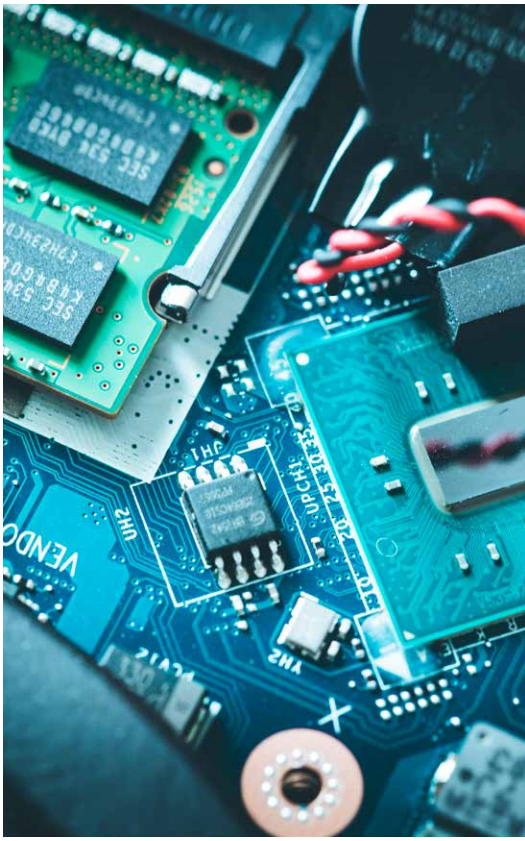
in einer anderen Reihenfolge als der Programmierer definiert hat durchzuführen. Wir Menschen gehen hier ganz ähnlich vor, wenn wir beispielsweise bei einem Kochrezept bestimmte Schritte früher oder später erledigen als sie im Rezept beschrieben sind. Diese natürlichen Optimierungen führen aber auch zu Sicherheitsproblemen.

Eine neue Klasse von Cyber-Angriffen, die wir an der TU Graz entdeckt und erforscht haben, sind transiente Angriffe wie Spectre, Meltdown, Zombie-Load oder Load Value Injection. Diese Angriffe nutzen aus, dass der Prozessor, beispielsweise durch das Verdrehen der Arbeitsschrittreihenfolge, Arbeitsschritte durchführt die er nicht durchführen sollte. Dabei kann der Prozessor auf geheime Daten, wie z.B. Passwörter, zugreifen. Den Fehler bemerkt der Prozessor und macht diese Arbeitsschritte vollständig rückgängig. Allerdings kann ein Angreifer den zuvor beschriebenen Caching Mechanismus verwenden, um abhängig von den geheimen Daten unterschiedliche Sachen in das Kurzzeitgedächtnis zu laden. Daraus was nun im Kurzzeitgedächtnis ist, kann der Angreifer ablesen was das Geheimnis war.



Bei Spectre nutzt der Angreifer aus, dass der Prozessor eine Vorhersage macht was wohl der nächste Arbeitsschritt ist und leider falsch liegt. Bei Meltdown und ZombieLoad nutzt der Angreifer aus, dass der Prozessor Arbeitsschritte ausführt, die er gar nicht ausführen dürfte und dadurch Daten liest, die er gar nicht lesen können sollte. Beim neuen Load Value Injection Angriff drehen wir Meltdown oder ZombieLoad um und sorgen dafür, dass ein anderes Programm unsere Daten liest – die es gar nicht lesen können sollte – und mit diesen falschen Daten weiterarbeitet. In allen Angriffsvarianten landen dann die Geheimnisse vom anderen Programm beim Angreifer, der diese dann beliebig weiterverarbeiten oder verschicken kann.

Derzeit gibt es noch keine absoluten Gegenmaßnahmen gegen sämtliche Angriffe und weitere Forschung im Themengebiet wird längerfristig nötig sein, um die Problematik vollumfassend in den Griff zu bekommen.
Gegen viele Angriffsvarianten helfen Software Patches, allerdings oft auf Kosten von Geschwindigkeit und Effizienz, gegen andere hilft neue Hardware, die von bestimmten Sicherheitsproblemen (z.B. Meltdown) nicht mehr betroffen ist. Die TU Graz steht mit den Hardwareherstellern in engem Kontakt, um sowohl Software als auch Hardware gegen die von uns entdeckten Angriffe sicher zu machen.



Ass. Prof. Dr. techn. Daniel Gruss

Assistant Professor für Cyber-Sicherheit
Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie
TU Graz

Eine A-SIT-Mitgliedschaft

Perspektiven der Donau-Universität Krems

Seit 2001 befasst sich das „Department für E-Governance in Wirtschaft und Verwaltung“ an der Donau-Universität Krems mit „E-Government“. Dieses Thema wurde 2001 erstmals als Forschungsprojekt für den Österreichischen Gemeindebund realisiert und als digitale Verwaltungsplattform „Kommunalnet.at“ im Jahr 2004 vorgestellt. 16 Jahre später bedient die Plattform 92% aller österreichischen Gemeinden und hat sich als unverzichtbares Werkzeug der österreichischen Kommunalverwaltung etabliert.

„Im Zusammenwirken mit A-SIT versuchen wir, über gemeinsame Projekte die forschungsgeleitete Lehre zu verstärken und das Bewusstsein für sicherheitsrelevante Themen zu erhöhen.“

Ebenfalls 2001 wurde parallel zur Forschungsaktivität die Lehre im Bereich E-Government ausgebaut und der erste E-Government Lehrgang angeboten. Da die digitale Entwicklung und damit die Übermittlung und Speicherung von Daten in der Verwaltung, im Handel, der Industrie sowie im Gesundheitswesen zu Beginn des neuen Jahrtausends eine massive Entwicklung nahm, die sich im Lauf der Jahre beschleunigte, wurde das Zentrum für Infrastrukturelle Sicherheit gegründet und 2001 der erste Lehrgang für „Information Security Management“ angeboten.

In der Zwischenzeit hat sich das Leistungsspektrum stark erweitert. Mit rund 30 Mitarbeiterinnen und Mitarbeitern forschen und lehren wir zu den Auswirkungen des digitalen und gesellschaftlichen Wandels auf Strategie, Organisation und Prozesse. Die Schwerpunkte des Departments gliedern sich in E-Government/E-Governance, Digitale Beteiligung und Kooperationsmodelle, Informationssicherheit zur Sensibilisierung für sich verändernde sozio-technische und rechtliche Governance-Strukturen sowie Sicherheitsforschung, vor allem in den Bereichen Cyber-Sicherheit, innovative Informations- und Kommunikations-

technologien sowie Sicherheitsmanagement.

Es ist die enge Verknüpfung mit dem Praxisleben der Studierenden, die für den Transfer von aktuellen Fragestellungen aus der Praxis in die Wissenschaft sorgt. Die entsprechenden Forschungsergebnisse werden wiederum über die Lehre und die Studierenden in die Gesellschaft getragen. Durch den permanenten Dialog mit unseren Absolventinnen und Absolventen über Wissenschaftskonferenzen, Kamingespräche und Alumni-Vorlesungen versuchen wir, einen Wissens-Kreislauf zu unterstützen.

„Ebenso wie die Digitalisierung ist das Konzept von Sicherheit so vielgestaltig wie die Gesellschaft selbst."

Ebenso wie die Digitalisierung ist das Konzept von Sicherheit so vielgestaltig wie die Gesellschaft selbst. Globalisierte Arbeits- und Wirtschaftsformen, Terror, Migrationsbewegungen und Digitalisierung verändern das gewohnte Gefüge, schaffen neue Bedingungen und verursachen Unsicherheit. Die Lösung dieser Herausforderungen kann nur durch Vertrauen und somit letztendlich durch konstruktiven Dialog gelingen.

Im Zusammenwirken mit A-SIT versuchen wir über gemeinsame Projekte die forschungsgeleitete Lehre zu verstärken und das Bewusstsein für sicherheitsrelevante Themen zu erhöhen.

Prof. Dr. Peter Parycek
Prof. Dr. Walter Seböck

Leitung Department für E-Governance in Wirtschaft und Verwaltung
Donau-Universität Krems

Mit seinem ganzheitlichen und herstellerneutralen Ansatz ist das BSI das Kompetenzzentrum für Cyber-Sicherheit in Deutschland.
Die Allianz mit A-SIT bringt innovativen Know-How-Austausch auf den Boden. Demzufolge verstehen wir uns als Gestalter und Vordenker im digitalisierten Zeitalter."

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

CERT.at
Erste Hilfe/Meldestellen, Hotlines

Mag. Otmar Lendl

Senior Information Technology Security Analyst
CERT.at

Bei Cyber-Angriffen und Aspekten der IT-Sicherheit mit Österreichbezug ist Ihr CERT.at als nationales Cyber Emergency Response Team der erste Anlaufpunkt. Allerdings ist CERT.at kein üblicher Helpdesk. Auf welchen Wegen sind Meldungen von Sicherheitsvorfällen im Alltagsbetrieb möglich? Können sich auch Behörden und Institutionen an Sie wenden?

Wir sind primär eine Informationsdrehscheibe und bewältigen für Unternehmen operativ keine Sicherheitsvorfälle. Um Incident-Reports (reports@cert.at) zu melden oder für Anfragen (team@cert.at) bevorzugen wir E-Mails. Die Kontaktierung gemäß NISG ist mit dem Formular auf https://nis.cert.at möglich. Alternativ erreichen Sie uns auch unter +43 1 5056416 78. Für Behörden ist das GovCERT (https://govcert.gv.at/) zuständig.

„IT-Sicherheit braucht einen ganzheitlichen Ansatz", ist Ihr Leitbild. Im nationalen CERT Österreichs leisten Sie täglich unermüdlich und gerne Erste Hilfe. Wie ist dies an einem Fallbeispiel zu veranschaulichen?

Wir hatten am 8. Mai 2020 ein gutes Beispiel, wie das funktioniert: Auf vielen Kanälen haben uns Meldungen über DDoS-Angriffe erreicht. Das ging von Anrufen direkt bei CERT-Mitarbeitern, E-Mails auf Mailinglisten der Netzbetreiber, Meldungen an Branchen-CERTs bis hin zu offiziellen Meldungen nach dem NISG. So entstand schnell ein Lagebild mit passenden Handlungshinweisen für alle Betroffenen.

Sie vernetzen CERTs und CSIRTs (Computer Security Incident Response

Teams). Darüber hinaus veröffentlichen Sie bei CERT.at Warnungen, Alerts und Tipps für Unternehmen. Wie ist die Struktur der CERT bzw. CSIRT-Landschaft aufgebaut?

Die Vertrauensgrundlage im IT-Sicherheitsbereich ist der kooperative Austausch über Vorfälle und den daraus gewonnenen Erkenntnissen. Möglich ist dies durch die Vernetzung mit anderen CERTs in Österreich, der operativen Koordinierungsstruktur laut NIS-Gesetz und dem Austrian Trust Circle. International gibt es bilaterale Kooperationen, in Europa das historisch gewachsene TF-CSIRT und das durch die NIS-Direktive geschaffene CSIRTs Network. Weltweit sind die CERTs im Rahmen der FIRST, dem globalen CERT-Verband organisiert.

„Weltweit sind die CERTs im Rahmen der FIRST, dem globalen CERT-Verband organisiert."

> *„Der Schutz am Perimeter, dem Übergang zum Internet, alleine reicht nicht aus."*
> *FH-Prof. DI Dr. Klaus Gebeshuber*

Wie viele sicherheitsrelevante Vorkommnisse bearbeiten Sie durchschnittlich pro Jahr? Lassen sich aus Ihren gemessenen Kennzahlen Trends zu steigenden Bedrohungen am Digitalisierungs- bzw. Wirtschaftsstandort Österreich ableiten?

Wir bearbeiteten im letzten Jahr 59.329 Kontaktaufnahmen durch Betroffene. Davon waren 7.757 Fehlalarme (13%) und 2.046 relevante Incidents (3,4% z.B.: DDoS-Attacken) sowie 11.081 relevante Incident-Reports (18,7%). Daraus ist im Vergleich zu 2018 bei relevanten Incident-Reports eine Erhöhung um 4,27% ersichtlich und demzufolge steigende Angriffe.

In letzter Zeit waren gezielte Angriffe mittels Ransomware wie „Trickbot" oder „Ryok" in Österreich häufig zu beobachten. Aber solche Bedrohungen sind nicht neu. Welche Erkenntnisse sind auf die Zukunft umlegbar und mit welchen Angriffen rechnen Sie in den kommenden Jahren? Wie ist Schutz für Behörden möglich?

Die ersten Ansätze zur IT-Absicherung waren Abwehr durch Perimeter (z.B.: Firewalls), um Systeme vom Internet abzuschotten sowie Erkennen von Eindringlingen (z.B.: SIEM).

Ich erwarte künftig mehr Fokus im Bereich „Überlebensfähigkeit". Wenn Angreifer weder abgewehrt, noch erkannt werden können und diese Daten verschlüsseln, folgt die Frage: „Wie gut sind Notfallsprozesse, die Backups und die Fähigkeit, mit schweren Störungen umzugehen?". Demzufolge sind geeignete Business-Continuity-Maßnahmen notwendig.

IT-Sicherheit und Deep Learning

NEURONALE NETZWERKE UND IHR SICHERER EINSATZ IN IT-LÖSUNGEN

Das Potential der Anwendung von neuronalen Netzwerken (Deep Learning) wurde in den letzten Jahren in unterschiedlichen Anwendungsgebieten sehr erfolgreich demonstriert. Vor allem im Bereich „Autonomes Fahren" ist der Einsatz neuronaler Netzwerke essenziell. Die Effektivität dieser neuen Technologie in diesem Bereich wird durch diverse aktuelle Beispiele und erste signifikante Erfolge eindrucksvoll belegt.

Allerdings bringt der breite Einsatz von neuronalen Netzwerken – vor allem in Bereichen, bei denen die Sicherheit und Gesundheit von Menschen von dieser Technologie abhängen – auch signifikante Herausforderungen mit sich. Diese betreffen unter anderem wesentliche Fragen zur Gewährleistung der organisatorischen und technischen Sicherheit im Rahmen der Erstellung entsprechender Softwarelösungen.

Im Bereich der klassischen Softwareentwicklung existieren seit Jahren etablierte Methoden zur Erhöhung der Sicherheit, die die Wahrscheinlichkeit eines erfolgreichen Angriffs minimieren. Beispiele dafür sind die Einhaltung von Standards für sichere Softwareentwicklung, die Etablierung eines ISMS, das Durchführen von Sicherheitsüberprüfungen in Form von Blackbox-/Whitebox-Tests oder auch der gezielte Einsatz von Kryptographie. Bei neuronalen Netzwerken können viele der bekannten Methoden aus der klassischen Softwareentwicklung nicht angewendet werden oder haben keine Wirkung. Beispielsweise ist der Einsatz von White-Box-Tests bei neuronalen Netzen im Vergleich zu klassischem Quellcode nicht möglich. Zum einen würden die Methoden und Ressourcen fehlen, um die Korrektheit von z.B. 20.000 Stunden an Video-Trainingsmaterial für ein Netzwerk zu überprüfen. Zum anderen führen unterschiedliche Parameter beim Trainieren des neuronalen Netzwerks sowie unterschiedliche Netzwerkstrukturen zu anderen Ergebnissen. Die Durchführung klassischer White-Box-Tests ist daher in vielen Fällen weder möglich noch zielführend. Für Softwarelösungen, die

> „Im Bereich der klassischen Softwareentwicklung existieren seit Jahren etablierte Methoden zur Erhöhung der Sicherheit."

auf neuronalen Netzwerken beruhen, müssen daher neue Methoden erarbeitet werden, um bereits in der Entwicklung dieser Lösungen deren Sicherheit gewährleisten zu können.

Eine weitere Herausforderung im Zusammenhang mit der Verwendung neuronaler Netzwerke in sicherheitskritischen Anwendungsszenarien stellen sogenannte „Adverserial Attacks" dar. Dabei versucht ein Angreifer Input-Werte zu finden, die das Ergebnis der Anwendung des Netzwerkes auf diese Input-Werte gezielt beeinflussen. Ein Beispiel aus dem Bereich „Autonomes Fahren" wäre das Anbringen von bestimmten Mustern auf einer Stopp-Tafel. Während diese Muster für den Menschen unscheinbar sind, können sie das neuronale Netzwerk dazu bringen, ein gänzlich anders Verkehrszeichen zu erkennen.

Die Folgen können drastisch sein. Problematisch ist hierbei, dass für das Finden eines passenden Musters der Zugriff auf das trainierte Netzwerk selbst gar nicht notwendig ist. Passende Muster können auch durch das Trainieren eines zweiten Netzwerks, das sich ähnlich wie das attackierte Netzwerk verhält, erreicht werden. Zum Schutz gegen solche Angriffe reicht es also zum Beispiel nicht, ein trainiertes Netzwerk vor direktem Zugriff zu schützen, da bereits allein das Beobachten des Verhaltens des Netzwerks für einen Angriff ausreichend ist.

Diese Beispiele zeigen, dass im Bereich IT-Sicherheit bei der Anwendung von neuronalen Netzwerken neue technische und organisatorische Vorgehensweisen notwendig werden. Etablierte Methoden zur Gewährleistung der Sicherheit von Softwarelösungen sind auf diese neue mächtige Technologie nur beschränkt anwendbar und stoßen in der Praxis bald an ihre Grenzen. Forschung zu IT-Sicherheit im Kontext neuronaler Netzwerke ist daher essenziell, um die nötige Sicherheit bei der Anwendung dieser mächtigen Technologie auch in sicherheitskritischen Anwendungsbereichen garantieren zu können.

Dr. Peter Teufl
CEO
A-SIT Plus GmbH

Mag. Vinzenz Heußler
Leiter des strategischen
NIS-Büros

Cyber-Security und Cyber-Resilienz

Cyber-Security und Cyber-Resilienz müssen in Österreich ein Selbstverständnis sein. Daher brauchen wir starke Brücken zwischen unserer Gesellschaft, dem Staat, den Unternehmen sowie mit der Wissenschaft und Forschung.

Das NISG fördert die Verbesserung der Cyber-Sicherheit in Österreich durch die Umsetzung der NIS-Richtlinie und die Ermöglichung eines kooperativen Informationsaustauschs als Erfolgskriterium für die Stärkung der Cyber-Security in Österreich.

TOPIC 4

Forschung

Security-Ausbildung

IT-Sicherheit
Herausforderung & Chance

Datendiebstähle sind neben anderen Cybergefahren heutzutage allgegenwärtig und werden immer gefährlicher. Unternehmen verlieren immer häufiger besonders wertvolle Daten. Das geht oft mit existenzbedrohenden Folgen einher und schadet somit auch dem österreichischen Digitalisierungs- bzw. Wirtschaftsstandort.

Online-Erpresser verschlüsseln Computer und Dokumente sogar von Kleinbetrieben. Besonders brisant wird es, wenn sensible Daten betroffen sind. Im Jahr 2020 erlitten 57 Prozent der österreichischen Unternehmen einen Cyberangriff. 2016 gab rückblickend lediglich die Hälfte an, Opfer einer Cyberattacke gewesen zu sein (49 Prozent). Kaum ein Unternehmen kam in den letzten Jahren an Attacken wie Spamproblemen, Virenangriffen, Ausfällen von IT-Systemen oder Datenverlusten sowie Ransomware-Angriffen vorbei. Das Bewusstsein der Unternehmen für die Gefahr, die Cyberkriminalität darstellt, ist in den letzten Jahren jedoch gestiegen. Groß ist aber oft noch die Unsicherheit, auf welche Schutzmaßnahmen man setzen sollte. Hier ist externe Beratung zur Orientierung ganz besonders wesentlich.

Externe Beratung immer öfter gefragt

Phishing und Malware sind und bleiben die häufigsten Angriffsarten in der virtuellen Welt, das ergibt die Studie der KPMG, welche in Kooperation mit dem KSÖ herausgegeben wurde. Knapp 74 Prozent der Cyberattacken sind in die Kategorie Phishing einzuordnen und 48 Prozent der Unternehmen wurden durch Malware-Attacken angegriffen. Rund 49 Prozent der Befragten gaben an, im Zuge der Attacke einen finanziellen Schaden unter EUR 10.000 erlitten zu haben. Darüber hinaus bestätigten 4 Prozent der Befragten, der finanzielle Schaden liege bei EUR 500.000 oder darüber – verursacht durch Unterbrechungen der Betriebsprozesse oder gar einen geschäftsschädigenden Imageverlust. Immerhin 36 Prozent der Unternehmen können den verursachten finanziellen Schaden gar nicht beziffern. Die Ergebnisse der Studie machen die Brisanz des Themas deutlich. Trotzdem wird Cybersicher-

> „Die Antwort auf die Herausforderungen im Bereich Cybersicherheit sind Österreichs IT- & Digitalisierungsberaterinnen und -berater, die Sicherheitslücken im IT-Bereich aufdecken und beheben, um geeignete Schutzmaßnahmen auszuwählen und diese praxistauglich umzusetzen."

heit oftmals wegen der Komplexität und der Vielschichtigkeit möglicher Problemlösungen zu wenig Bedeutung beigemessen. Die Antwort auf die Herausforderungen im Bereich der Cybersicherheit sind Österreichs IT- & Digitalisierungsberaterinnen und -berater, die Sicherheitslücken im IT-Bereich aufdecken und beheben, geeignete Schutzmaßnahmen auswählen und diese praxistauglich umsetzen. Aber genau das setzt das nötige Fachwissen voraus.

„Als ausgewiesener „Certified Data & IT Security Expert" kann man am Markt noch überzeugender auftreten sowie auf das notwendige Rüstzeug zurückgreifen, um den Herausforderungen in der IT-Sicherheit zu begegnen. Diese Form der Weiterbildung macht eben in jeder Hinsicht sicher."

Wissen zu IT-Sicherheit und Datenschutz vertiefen

Die UBIT-Akademie incite stimmt ihr Leistungsprofil auf die Herausforderungen der Digitalisierung ab. Der Lehrgang „Data & IT Security" vermittelt Fachwissen in den Bereichen IT-Risikomanagement und Netzwerksicherheit. Der Lehrgang wurde in Zusammenarbeit mit dem Innenministerium und SBA-Research, der Österreichischen Computergesellschaft (OCG), dem Zentrum für sichere Informationstechnologie Austria (A-SIT), dem Kuratorium Sicheres Österreich (KSÖ) und der UBIT-Experts Group IT-Security entwickelt. Denn: Eine zielgerichtete Security-Ausbildung ist eine zentrale Säule für einen starken Digitalisierungs- bzw. Wirtschaftsstandort Österreich.

Gerade in diesem neuralgischen Bereich macht es sich auch bezahlt, nicht nur den Lehrgang zu absolvieren, sondern auch die Zertifizierung anzustreben. Als ausgewiesener „Certified Data & IT Security Expert" kann man am Markt noch überzeugender auftreten und auf das notwendige Rüstzeug zurückgreifen, um den Herausforderungen in der IT-Sicherheit zu begegnen. Diese Form der Weiterbildung macht eben in jeder Hinsicht sicher.

KR Mag. Alfred Harl, MBA CMC

Obmann des Fachverbandes UBIT der WKO

Security-Ausbildung an der TU Graz

Univ.-Prof. Dr. Stefan Mangard

Institutsvorstand IAIK,
TU Graz

Sie leiten das Institut für angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) an der TU Graz. Ihr Institut bietet Lehrveranstaltungen im Bereich der Security sowohl auf Bachelor-Ebene, für Master-Studierende als auch für Studierende in Ihrem PHD-Programm „Doctoral School of Computer Sciences" an. Wie können potentielle Arbeitgeber wie etwa Behörden das Profil der Absolventinnen bzw. Absolventen einstufen?

Auf Bachelor-Ebene bieten wir mit einer einführenden Vorlesung zur Informationssicherheit jene Grundlagen, die heutzutage jeder Informatiker kennen soll oder muss. Die wirkliche Vertiefung erfolgt dann in den Masterstudien. Hier haben wir einen neuen Schwerpunkt „Information Security" geschaffen. Die Studierenden werden in den Kernthemen Cryptology & Privacy, System Security, Formal Methods und Secure Applications ausgebildet. Der gesamte Katalog wird übrigens in Englisch unterrichtet und ist damit auch international attraktiv. Am Beispiel Behörden als Arbeitgeber dürfen diese von einer Absolventin etwa erwarten, dass sie aus dem Kernthema Secure Applications bereits Kenntnisse zu sicheren Prozessen und E-Government mitbringt.

Auch waren Sie sehr intensiv in die Entstehung des „Cyber Security Campus" und der damit verbundenen, starken Kooperation mit SGS für einen herausragenden Wissenstransfer involviert. Damit wurde ein weltweit einzigartiger Ort als innovativer Hub für Forschung, Ausbildung, Prüfung und Zertifizierung erschaffen. Wodurch zeichnet sich diese Kooperation für die Security-Ausbildung an der TU Graz aus?

„Der gesamte Katalog wird übrigens in Englisch unterrichtet und ist damit auch international attraktiv."

Uns ist forschungsgestützte Lehre besonders wichtig, da wir überzeugt sind, dass die Ausbildung umso besser ist, je stärker die Lehrenden

ihr Wissen aus Forschungsaktivität am Puls des Standes der Wissenschaft schöpfen. Wir sind deshalb auf den Cyber Security Campus besonders stolz, da sich damit die zuvor schon hohe Forschungsintensität zur Informationssicherheit in Graz massiv erhöhen wird. Dies bildet die Basis, dass Studierende an aktuellen Themen ausgebildet werden, bietet ihnen aber auch die Chancen, das erworbene Wissen nach dem Studienabschluss bei potenten Arbeitgebern am Standort einsetzen zu können.

Cyber-Sicherheit steht an der TU Graz und insbesondere am IAIK seit vielen Jahren im Blickfeld der Forschung. Demzufolge sind die erzielten Resultate Ihrer Teams exzellent. Die Liste renommierter Publikationen ist unglaublich lang. Was sind die Vorteile, wenn derart geschätzte Forscherinnen und Forscher im Security-Bereich an der TU Graz lehren?

Die besten in einem Feld zu haben, die auch international aufsehenerregendes wie Meltdown oder Spectre erforschen oder Wettbewerbe zur Kryptographie gewinnen, dabei obendrein sehr gute Lehrende sind, ist für Studierende natürlich immens attraktiv. Es profitieren aber nicht nur die Studentinnen und Studenten, wir bekommen als Institut damit zum Thema Informationssicherheit motivierte junge Leute für Projekt- und Masterarbeiten und später für das Doktoratsstudium, die dann diesen Vorbildern oft ebenso erfolgreich nacheifern.

Im Studium können Studierende den sogenannten „Major Information Security“ auswählen. Was ist darunter vorstellbar und in welchen Bereichen können Absolventinnen bzw. Absolventen arbeiten und dort Werte für Organisationen stiften?

Das Major und Minor System erlaubt den Studierenden, sich flexibel in eine Richtung zu spezialisieren. Ist etwa das Interesse stärker in der Netzwerksicherheit, wird eine Studentin zum Wahlfachkatalog Information Security den Katalog Communications and Mobile Computing als Minor kombinieren, ist das Interesse in der Hardware, bietet sich die Kombination mit Microelectronics and IC Design an.

„1011“ Gründe für einen Security Master am IAIK

DER SECURITY MASTER AM IAIK DER TU GRAZ IST ÄUSSERST EMPFEHLENSWERT, WEIL...

- die Themengebiete so vielseitig sind, dass sich jeder Student nach seinen Vorlieben spezialisieren und seine Vorlesungen auswählen kann.
- der Unterricht sehr praxisorientiert ist und man die theoretischen Grundlagen auch sofort in Übungen umsetzen muss.
- man spannende Übungen und Vorlesungen absolviert, bei denen man von der Begeisterung der Vortragenden angesteckt wird.
- Tutoren und Lehrende stets bemüht sind, den Studenten bestmöglich zur Seite zu stehen und immer ein offenes Ohr für Fragen und Unklarheiten haben.
- die Vortragenden international führende Wissenschafter sind, die auf den Top-Konferenzen in ihren Gebieten publizieren.
- die Bachelor- und Masterarbeit in aktuellen Forschungsgebieten geschrieben werden kann und Studenten somit einen relevanten Beitrag zu aktueller Forschung leisten.
- Studenten im Zuge ihrer Bachelor-/Masterarbeit oder ihres Bachelor-/Masterprojekts an einer wissenschaftlichen Publikation mitarbeiten können, die auf international

angesehenen Konferenzen veröffentlicht wird.
- im Zuge der wissenschaftlichen Arbeiten mit namhaften Firmen zusammengearbeitet wird.
- der Beginn eines Doktoratsstudiums durch die frühe Integration der Studenten in die wissenschaftliche Arbeit erleichtert wird.
- der Security Bereich immer mehr an Bedeutung gewinnt, was sich in den ausgezeichneten Jobaussichten nach dem Abschluss widerspiegelt.
- am IAIK Leute arbeiten, mit denen es wirklich Spaß macht, sein Wissen zu erweitern und in den Security Bereich einzutauchen.

DI Angela Promitzer

Digitization Professional
August-Wilhelm Scheer Institut
Saarbrücken

Professional MSc Management & IT

Information-Security-Wandel gestalten

Wer die Herausforderungen und Chancen der digitalen Transformation meistern will, muss auch ein Stück weit neue Technologien und ebenso kritische Infrastrukturen verstehen. Die durch Krisen intensivierte Digitalisierung schafft neue Risiko- und Gefahrenpotentiale, denn immer mehr grundlegende (Geschäfts-) Prozesse basieren auf dem IT-Einsatz und der zugrundeliegenden IT-Infrastruktur. Damit rückt die sichere Datenverarbeitung und somit die Gewährleistung einer umfassenden Informationssicherheit immer mehr in das Zentrum strategischer Überlegungen und Managemententscheidungen.

„Sichere Datenverarbeitung rückt immer mehr ins Zentrum von Managemententscheidungen."

Die Studierenden gestalten den Wandel im Bereich der Information-Security, indem diese Zukunftskompetenzen durch den berufsbegleitenden Universitätslehrgang Professional MSc Management und IT – Spezialisierung Information Security Management aufbauen. Unsere AbsolventInnen sind Profis im Bereich der Informationssicherheit mit Expertise im Managementbereich und können somit mit sensiblen Veränderungen umgehen. Der Weiterbildungs-Lehrgang richtet sich an MitarbeiterInnen in Unternehmen sowie Behörden, die derzeit oder künftig Aufgaben im Bereich der Informationssicherheit wahrnehmen und in diesem Bereich eine fundierte Ausbildung mit universitärem Abschluss anstreben.

In vier Semestern vermittelt dieser Universitätslehrgang praxisbasierte Inhalte und wissenschaftlich fundierte Methoden für den zielgerichteten Einsatz der Informations- und Kommunikationstechnologien sowie für ein gesamtheitliches Management. Der Aufbau ist modular und didaktisch an die Bedürfnisse für ein berufsbegleitendes Studieren angepasst. Das Kerncurriculum bildet die Basis. Im 3. Semester werden die Spezialisierungsinhalte der Informationssicherheit vermittelt und das 4. Semester ist dem Finalisieren der Master-Thesis gewidmet. Anmeldungen für den Lehrgang sind auf der Webseite www.donau-uni.ac.at/ möglich.

Prof. Dr. Peter Parycek
Prof. Dr. Walter Seböck

Leitung Department für E-Governance in Wirtschaft und Verwaltung
Donau-Universität Krems

Master-Studium - Artificial Intelligence and Cybersecurity

Elisabeth Oswald

Univ.-Prof[in]. Dipl.-Ing[in]. Dr[in]. für Cybersecurity
Head of the Cybersecurity Research Group at AAU
D!ARC/AINF, AAU

Das englischsprachige Master-Studium „Artificial Intelligence and Cybersecurity" wird als sog. „Double-Degree-Program" zur Ausbildung internationaler Spezialistinnen bzw. Spezialisten angeboten. Was sind die Besonderheiten dieses Studiums und wovon profitieren die Studierenden insbesondere?

Vermittelt werden von einem breiten wissenschaftlichen Team gemeinsam mit der Universität Udine technische Inhalte zu den Themen AI und Cybersecurity sowie Fähigkeiten, um die sozialen, ethischen und rechtlichen Aspekte praktischer Umsetzungen zu analysieren. Studierende arbeiten im 2-jährigen Studienplan in Projekten sowie in klassischen Lehrveranstaltungen auch gemeinsam mit Industriepartnern.

Der inhaltliche Fokus liegt auf grundlegenden Techniken der Cybersecurity und der Artificial Intelligence, im Blickfeld deren Verknüpfung. Welche Inhalte lernen Absolventinnen bzw. Absolventen und welche Schwerpunkte können die Studierenden auswählen?

Studierende erlernen notwendige Grundlagen (z.B.: Logik, technische Sicherheit, ethische und rechtliche Aspekte) und können weitere Lehrveranstaltungen im Umfeld von AI bzw. Cybersecurity wählen. Wir bieten auch Speziallehrveranstaltungen in den Gebieten AI und Cybersecurity an. Deren Inhalte werden, basierend auf Wünschen der Studierenden und Lehrenden, von Jahr zu Jahr adaptiert.

Der internationale Austausch erfolgt vordergründig mit der Università degli studi di Udine. Was sind die Vorteile für den Österreichischen Digitalisierungs- bzw. Wirtschaftsstandort durch diesen tollen Zugang?

Österreichische und internationale Studierende haben dank der Kooperation die Möglichkeit, eine Lehrveranstaltung in Udine zu absolvieren und Diversitätsaspekte im Projektalltag zu integrieren. Gleichzeitig bieten wir Lehrveranstaltungen für Studierende aus Udine an. Durch die Zusammenarbeit mit internationalen Industriepart-

nern möchten wir zu einer Drehscheibe in der Alpe-Adria-Region werden, die Unternehmen bzw. Institutionen, die Expertise im Bereich AI/Cybersecurity haben oder benötigen, vernetzt.

In welchen Bereichen können Absolventinnen bzw. Absolventen in Behörden, Unternehmen oder anderen Organisationen später arbeiten und wertvolle Beiträge am Österreichischen Digitalisierungs- bzw. Wirtschaftsstandort leisten?

Absolventinnen des Studiums sind für Beschäftigungsfelder geeignet, in denen Expertise in AI bzw. Cybersecurity gebraucht werden. Herausragend ist die Ausbildung in beiden Kompetenzfeldern und die Einbringung von Erfahrungen aus dem Bereich „Responsible Innovation“ in relevante Projekte. Das ist bis dato nicht nur in Österreich einzigartig, es ist auch notwendig, um den Anforderungen von Ethical AI gerecht zu werden.

Herausragend ist die Ausbildung in beiden Kompetenzfeldern und die Einbringung von Erfahrungen aus dem Bereich „Responsible Innovation“ in relevante Projekte.

Der Bedarf an qualifizierten Spezialistinnen und Spezialisten ist in Österreich sehr groß. Allerdings, welche Grundvoraussetzungen sollten Studierende mitbringen und wem empfehlen Sie dieses Master-Studium auszuwählen?

Die Zulassung zum Studium ist für 30 Studienplätze pro Jahr durch ein Aufnahmeverfahren geregelt. In Frage kommen Bewerberinnnen und Bewerber, die ein mathematisches, technisches oder naturwissenschaftliches Studium abgeschlossen haben und Erfahrung mit Informatik mitbringen. Enthusiasmus, gute Noten im Erststudium und ein überzeugendes Motivationsschreiben sind die Grundlagen zum Erfolg im Aufnahmeverfahren.

Projekt ACySS
Aviation Cyber Security Study

EVALUIERUNG DER CYBER SECURITY IM BEREICH DER AVIONIC

Das Projekt „Aviation Cyber Security Study“ (ACySS)“ wurde im Rahmen der 12. FFG – Takeoff Ausschreibung mit Partnern aus der Industrie und dem Institut für Luftfahrt der FH JOANNEUM in Graz sowie dem Institut Internet-Technologien & – Anwendungen der FH JOANNEUM in Kapfenberg durchgeführt.

Im Zuge des Projekts wurde die IT-Security von Komponenten und Systemen in der Avionik untersucht. Das Ziel dabei war, Sicherheitsschwachpunkte sowohl in kritischen als auch unkritischen Netzwerkteilen aufzudecken, um gegebenenfalls Empfehlungen zur Vermeidung zu beschreiben.

Hierzu wurde ein Testbed, bestehend aus Avionic Netzwerkswitches mit Avionics Full-Duplex Switched Ethernet (AFDX) und Time-Triggered Ethernet (TTEthernet) Kompatibilität, sowie einem In-flight Entertainment (IFE) System aufgebaut. Auf Basis dieses Testbeds wurden Angriffsszenarien entwickelt und durchgeführt.
Der erste Teil der Studie befasst sich mit einer Risikoanalyse auf mehreren Ebenen, wobei Angriffsszenarien aus der Sicht eines gewöhnlichen Passagiers in der Kabine erfasst wurden.

Die erste Ebene befasst sich mit der Möglichkeit des physischen Zugriffs, um in das Avioniknetzwerk einzudringen. Hierzu wurden, in Kooperation mit Experten der Flugzeugwartung, Möglichkeiten diskutiert und eruiert. Die zweite Ebene behandelt die technischen Angriffsmöglichkeiten anhand des erstellten Testbeds. Der zweite Teil des Projekts behandelt die technischen Untersu-

„Bei der durchgeführten Studie wurden mehrere mögliche Schwachstellen auf Softwareebene, sowie auf Netzwerkebene aufgedeckt.“

chungen von Netzwerkkomponenten sowie des IFE.

Für die Analyse der Netzwerkkomponenten wurden dazu verschiedene Angriffsszenarien entwickelt, um die Komponenten auf Stress, Protokollverletzungen sowie Umweltfaktoren zu testen. Die Untersuchung des IFE umfasste statische Analyse der eingesetzten Software sowie die dynamische Analyse des Netzwerkverkehrs. Bei der durchgeführten Studie wurden mehrere mögliche Schwachstellen auf Softwareebene sowie auf Netzwerkebene aufgedeckt.

Diese Möglichkeiten dienten in weiterer Folge zur Diskussion über Maßnahmen zur Vermeidung von Angriffen. Die gefundenen Schwachstellen und der Fakt, dass immer mehr IT-Systeme auch in der Avionik Einzug finden, bestärken die potenzielle Gefahr, die von Angriffen auf diese Systeme ausgeht.
Daher sollten bereits Hersteller besonders darauf achten, state-of-the-art Sicherheitslösungen zu integrieren, sowie Upgrade Möglichkeiten bestehender Systeme bedenken.

„Es sollten bereits Hersteller besonders darauf achten, state-of-the-art Sicherheitslösungen zu integrieren, sowie Upgrade Möglichkeiten bestehender Systeme bedenken“

Die fortschreitende Digitalisierung und Integration neuer IT-Systeme stellt heutzutage viele Bereiche vor neue Herausforderungen. Lag am repräsentativen Beispiel der Avionik der Fokus etwa bisher primär auf Verfügbarkeit und Ausfallssicherheit, müssen Risikoanalysen in diesem Bereich künftig auch spezifische Bedrohungsszenarien aus der IT-Domain berücksichtigen. Dank domainübergreifender Risikobetrachtungen sind langjährige Erfahrungen aus der Avionik mit aktuellen Best Practices aus dem Bereich der IT-Sicherheit gezielt kombinierbar, sodass auch in Zukunft ein hohes Maß an Sicherheit gewährleistet werden kann.“

Dr. Thomas Zefferer, Senior IT-Security Expert A-SIT Plus GmbH

DI Dr. Klaus Gebeshuber

FH-Prof. für IT-Security
Institut Internet-Technologien & - Anwendungen,
Studiengang IT & Mobile Security, FH JOANNEUM Kapfenberg

Cyber-Security-Studium an der FH St. Pölten

FH-Prof. Mag. Dr. Simon Tjoa

Studiengangsleiter
Department Informatik und Security, FH St. Pölten

Das neue Master-Studium „Cyber Security and Resilience" bildet seit Oktober-2020 an der FH St. Pölten ein einzigartiges Fundament zur englischsprachigen Ausbildung für internationale Spezialistinnen bzw. Spezialisten im Bereich der Absicherung moderner, digitaler Infrastrukturen. Wovon profitieren Studierende und Behörden bzw. Unternehmen mehrheitlich?

Der neue Studiengang vermittelt Bachelor-AbsolventInnen von Informatikstudien die notwendigen Kompetenzen, um sichere, widerstandsfähige Informationssysteme und digitale Services zu entwickeln, zu betreiben und zu verbessern.

Modernste Infrastruktur (z.B.: Remotezugriff auf alle Labore rund um die Uhr, Cyber Defence Center zu Übungszwecken), neue Lehrmethoden (z.B.: Blockunterricht, Game-based Learning) und praxisnahe Inhalte (z.B.: duale Projekte) bieten eine ideale Lernumgebung für Studierende. Unternehmen profitieren durch die Ausbildung neuer, dringend benötigter Fachkräfte. Durch duale Projekte ist es Unternehmen möglich, Studierende schon während des Studiums näher kennenzulernen. Sie können weiters ihre individuellen Themen aktiv in das Studium zur Abarbeitung einbringen und haben dadurch nicht nur den Vorteil, an der Ausbildung der Studierenden mitzuwirken, sondern auch aktuelle Thematiken mit Hilfe der Mentor*innen und Studierenden fundiert zu bearbeiten.

Angeboten wird ein duales Vollzeitstudium. Welche Besonderheiten können Sie insbesondere für das duale Studium hervorheben, da dieser Modus verglichen mit Deutschland bei uns noch nicht sehr weit verbreitet ist und was verändert sich dadurch im Bereich der IT-Security-Ausbildung?

Das duale Studium ist in vielen europäischen Ländern, wie beispielsweise Deutschland schon ein Erfolgsmodell. Dabei werden Studium und Beruf enger verzahnt als in herkömmlichen berufsbegleitenden Studiengängen. Praxis- und Ausbil-

dungsblöcke in kooperierenden Unternehmen sind fixe Bestandteile des Curriculums und ermöglichen Studierenden, gelernte Inhalte frühzeitig in der Praxis umzusetzen und zu festigen. Im Studiengang Cyber Security and Resilience geschieht dies in drei dualen Projekten in Unternehmen, welche durch intensives Mentoring seitens der FH unterstützt wird. Dies bietet nicht nur gute Studienbedingungen, sondern steigert auch die Übernahme- und Arbeitsmarkt-Chancen enorm.

„Das duale Studium ist in vielen europäischen Ländern, wie beispielsweise Deutschland schon ein Erfolgsmodell."

Der Internationale Fokus wird beispielsweise auch durch Austauschsemester an weltweit ansässigen Partner-Universitäten untermauert. Was sind die Vorteile für den Österreichischen Digitalisierungs- bzw. Wirtschaftsstandort durch diesen Zugang?

Die internationalen Kooperationen des Department Informatik und Security der FH St. Pölten mit weltweit führenden Hochschulen (z.B.: Pennsylvania State University, Sungkyunkwan University oder Norwegian University of Science and Technology) ermöglichen eine Vielzahl von Chancen für Studierende (z.B.: Summer Schools, Austauschsemester, Gastvorträge). Hierbei steht vor allem eine internationale Vernetzung mit Opinion Leadern der Zukunft im Fokus.

Wie wird meine Behörde oder mein Unternehmen Ihr dualer Partner und welche Voraussetzungen sind zu erfüllen? Welche Kosten entstehen für unsere Organisation und kann ein Betreiber wesentlicher Dienste laut NISG ebenfalls dualer Partner werden?

Dualer Ausbildungspartner kann grundsätzlich jedes Unternehmen werden, in denen Studierende in dualen Security-Projekten mitarbeiten können. Interessierte Unternehmen beraten wir gerne in persönlichen Gesprächen oder per Email. Sollte ein Unternehmen interessiert sein, dualer Partner zu werden oder weitere Informationen benötigen, bitten wir um ein kurzes Mail an Bettina Mainunsch (bettina.mainusch@fhstp.ac.at).

Warum sollte sich eine Informatik Absolvent*in gerade für den neuen Master Cyber Security and Resilience entscheiden?

In diesem englischsprachigen Studium erhalten Absolvent*innen neben umfassenden Kompetenzen im Bereich der Software-, Betriebssystem- und Netzwerksicherheit auch umfassende rechtliche und ethische Grundlagen, sowie Know-How im Umgang mit neuen Technologien (zB KI). Kurzgefasst – alles, um einen wesentlichen Beitrag für die Gewährleistung von Cybersicherheit in nationalen und internationalen Unternehmen zu gewährleisten.

TOOP
The Once-Only Principle Project

ZEIT- UND KOSTENERSPARNISSE DURCH DIE REDUKTION VON ADMINISTRATIVEN AUFWÄNDEN BEI RECHTLICHEN AUFLAGEN

Das Projekt „TOOP" wurde im Januar 2017 von der Europäischen Kommission als eine Initiative von rund 50 Organisationen aus 20 EU-Mitgliedstaaten und assoziierten Ländern ins Leben gerufen. Das Hauptziel von TOOP besteht darin, das „Once-Only Principle" grenzüberschreitend zu erforschen und zu demonstrieren, wobei der Schwerpunkt auf Daten von Unternehmen liegt. Auf diese Weise will TOOP einen besseren Austausch von geschäftsbezogenen Daten oder Dokumenten mit und zwischen öffentlichen Verwaltungen ermöglichen und den Verwaltungsaufwand sowohl für Unternehmen als auch für öffentliche Verwaltungen verringern. Um das gesteckte Ziel zu erreichen, realisiert TOOP die Umsetzung von 3 nachhaltigen Piloten durch die Verwendung einer paneuropäischen, föderativen, grenzüberschreitenden IT-Architektur.

Auf diese Weise werden Register als auch e-Government Architekturen in ganz Europa verbunden. Die entwickelte Umsetzung berücksichtigt und integriert dabei existierende Systeme der EU-Mitgliedstaaten sowie assoziierter Länder. Mit Hilfe von TOOP profitieren Unternehmen in ganz Europa durch die Reduktion von administrativen Aufwänden bei der Erfüllung von rechtlichen Auflagen in Form von Zeit- und Kostenersparnissen. Gleichzeitig behalten die Unternehmen die Kontrolle über Ihre Daten während des Austauschs mit der öffentlichen Verwaltung; gemäß den Vorgaben der EU-Datenschutzrichtlinie.

Darüber hinaus ermöglicht TOOP auch der öffentlichen Verwaltung, durch die Reduktion der verwaltungstechnischen Hürden, ebenfalls effizienter und kostensparender zu agieren und darüber hinaus ihre Serviceleistungen gegenüber den Unternehmen weiterzuentwickeln und zu optimieren. Dies führt letztendlich zu einer Etablierung eines besser funktionierenden Digital Single Market mit höherer KundInnenzufriedenheit und zu einem besseren Ansehen der öffentlichen Verwaltung.

Prof. Dr. Thomas J. Lampoltshammer

Stv. Leiter Zentrum für E-Governance
Donau-Universität Krems

Security & Privacy an der TU Wien

Symbiose aus Forschung, Entwicklung und Lehre

Der Forschungsbereich Security & Privacy an der TU Wien kombiniert formale Methoden mit angewandter Sicherheitsforschung. Das Team umfasst Prof. Matteo Maffei, Prof. Georg Fuchsbauer, und Prof. Martina Lindorfer, sowie ein wachsendes Team von derzeit 15 StudentInnen und PostDocs.

Vienna Cybersecurity and Privacy Research Center (ViSP)

Mit der Universität Wien und dem IST Austria wurde im Juni 2020 ViSP gegründet. Ziel ist es, die bisher in diesem Bereich aufgebauten Kompetenzen zu bündeln und international sichtbare Forschungsaktivität anzuregen. Weiters soll die Ansiedlung internationaler Firmen erleichtert und Ausbildungsangebote für Security-ExpertInnen erweitert werden. Interessierte StudentInnen erhalten zusätzlich Mentoring zur Gründung eigener Startups.

Ab Herbst 2020 wird die Spezialisierung Security & Privacy als Pilotprojekt im Masterstudium Software Engineering an der TU Wien angeboten. Ziel dieses Schwerpunktes ist es, AbsolventInnen zu ihrem Diplom eine Zusatzqualifikation in Security & & Privacy zu bescheinigen, wenn sie eine gewisse Anzahl von Lehrveranstaltungen aus diesem Bereich absolvieren. Das Vorlesungsangebot beinhaltet Themen aus den Bereichen Software- und Systemsicherheit, Formale Verifikation, Kryptographie, und Netzwerktechnik. Die konkreten Inhalte sind forschungsgetrieben und werden laufend mit neuesten Erkenntnissen aus der Forschung aktualisiert.

„Ziel dieses Schwerpunktes ist es, AbsolventInnen zu ihrem Diplom eine Zusatzqualifikation in Security & Privacy zu bescheinigen."

StudentInnen werden auch während der Abschlussarbeiten zum Bachelor und Master aktiv in den Forschungsbetrieb eingebunden, oft mit einer Mitarbeit an erstklassigen wissenschaftlichen Publikationen als Resultat.

Neben dieser Forschungs-Orientierung spielen auch Gamification und praktische Erfahrung in der Lehre eine große Rolle. Übungen sind im Stile von Capture-the-Flag (CTF) Turnieren konzipiert: Dabei können StudentInnen anhand von Challenges spielerisch praktische Erfahrung mit der Ausnützung und Verhinderung von Sicherheitslücken gewinnen. Zukünftig wird dieses Trainingsangebot auch auf Firmen ausgeweitet.

Prof. Dr. Matteo Maffei
Prof. Dr. Georg Fuchsbauer
Prof. Dr.in Martina Lindorfer

Fakultät für Informatik
Fachbereich Security & Privacy
TU Wien

IT & Mobile Security an der FH Joanneum in Kapfenberg

DI Dr. Klaus Gebeshuber

FH-Prof. für IT-Security
Institut Internet-Technologien & – Anwendungen,
Studiengang IT & Mobile Security, FH JOANNEUM Kapfenberg

Sie bieten das Master-Studium „IT & Mobile Security" am Standort Kapfenberg der FH Joanneum an, um neue innovative Wege im Themenkomplex der IT-Sicherheit zu finden. Welche Schwerpunkte werden im Rahmen dieses Studiums ausgebildet und wovon profitieren Studierende sowie Behörden bzw. vorwiegend auch Unternehmen ganz besonders?

Es handelt sich hierbei um ein technisches IT-Security Masterstudium, wobei die Security Aspekte im gesamten System-Entwicklungsprozess Berücksichtigung finden. Secure Software Design und Secure Development legen den Grundstein für eine solide, sichere und belastbare Basis. Egal, ob es sich hier um eine Anwendung auf einem Mobiltelefon, eine WEB-Applikation oder ein cloudbasierendes verteiltes System handelt, die grundlegenden Security Überlegungen müssen bereits im Fundament einfließen. Neben der sicheren Softwareentwicklung ist auch die Betriebsumgebung von Bedeutung, Lehrveranstaltungen mit Fokus auf Operating System Security, Database Security und Secure Server Environments decken diesen Bereich ab. Schlussendlich können fehlerhafte Konfiguration und der falsche Einsatz von Technologien zu Security Problemen führen. Die Überprüfung bestehender Systeme mit Methoden der Security Analyse bis hin zum Penetration Testing und Red Team Assessments sind ebenso Fokus des Studiums. Unsere Studierenden müssen die Methoden der Angreifer gut kennen, um sinnvolle Verteidigungsstrategien zu entwickeln. In Laborumgebungen werden dazu Systeme mit klassischen Hacking Methoden angegriffen und entsprechende Abwehrmaßnahmen implementiert.

Angeboten wird dieser Studiengang zum einen berufsbegleitend und andererseits als Vollzeitstudium. Wie können Studierende und Organisationen wie z.B.: Behörden oder Unternehmen die Organisation für das berufsbegleitende Studium einordnen? Welche Beiträge sind von Seiten der Unternehmen bzw. Behörden aber auch andererseits aus der Perspektive der Studierenden erforderlich, um

das Studium erfolgreich zu absolvieren?

Ein berufsbegleitendes Studium bietet den großen Vorteil, parallel zum ausgeübten Beruf zeitgleich eine akademische Ausbildung zu absolvieren. Zu beachten ist allerdings die zusätzliche Belastung durch Studieren am Abend und am Wochenende. Ein großer Teil des Studiums wird natürlich in Form von Online Einheiten angeboten, die sich um Präsenzeinheiten vor Ort mit praktische Übungen im Labor und Vorlesungen ergänzen. Ein berufsbegleitendes Studium erfordert eine große Disziplin und gutes Zeitmanagement. Die Arbeitswoche endet im Normalfall nicht am Freitag, sondern meist erst am Samstagabend. Wir empfehlen hier unseren Studierenden, wenn möglich, eine Reduktion der Wochenarbeitszeit um einige Stunden, um auch Zeit für Familie, zur Vorbereitung und Regeneration zu haben.

Vor dem Hintergrund der fortschreitenden Digitalisierung ist insbesondere die zunehmende Vernetzung einerseits Chance, aber andererseits auch ein Sicherheitsrisiko. Dieser Studiengang deckt vordergründig technische Aspekte der Sicherheit im Internet ab. Welche zentralen Eckpunkte zum Schutz vor Angriffen erlernen die Studierenden und wie können sich Behörden bzw. Unternehmen als potentielle Arbeitgeber das Profil der Studierenden vorstellen?

Ein Sicherheitskonzept muss auf mehreren Ebenen wirksam ein. Der Schutz am Perimeter, dem Übergang zum Internet, alleine reicht nicht aus. Dennoch ist die richtige Firewall-Konfiguration eine wichtige Aufgabe, wo sowohl eingehender als auch ausgehender Datenverkehr gesteuert wird. Typische Cyber Angriffe starten meist von infizierten Computern im internen Netzwerk, die als ersten Schritt eine Verbindung zum Angreifer im Internet aufbauen, deshalb ist auch die Betrachtung von ausgehendem Datenverkehr sehr wichtig. Unsere Studierenden lernen neben der Konfiguration von Firewalls auch das Design sicherer Netzwerke, die eine entsprechende Segmentierung, d.h., die Aufteilung in unterschiedliche Sicherheitszonen, aufweisen. Ein sauberes Sicherheitsdesign geht auch davon aus, dass sich ein Angreifer bereits im Netzwerk befindet. Um die Auswirken eines Angriffs im internen Netz zu erkennen und auch einzuschränken, sind lokale Firewalls, Intrusion Detection Systeme, Honeypots und Intrusion Prevention Systeme Teil einer Sicherheitsarchitektur. In praktischen Übungen werden Netzwerke ge-

„Ein berufsbegleitendes Studium bietet den großen Vorteil, parallel zum ausgeübten Beruf zeitgleich eine akademisch Ausbildung zu absolvieren.“

plant, aufgebaut, angegriffen und ebenso verteidigt. Auch die richtige Reaktion auf eine laufende Angriffssituation, die Incident Response, ist Teil der Ausbildung.

Der internationale Austausch mit Partneruniversitäten wird von Ihrem Studiengang bzw. Ihrem Institut forciert. Zu diesem Zweck bieten Sie Auslandssemester an. Welchen Nutzen haben Studierende bzw. deren Arbeitgeber wie etwa Behörden oder Unternehmen vor diesem Hintergrund? Welche Herausforderungen bestehen bei der Absolvierung der Auslandssemester?

Ein Auslandssemester bei einer unserer Partneruniversitäten ist auf alle Fälle zu empfehlen. Von den Erfahrungen kann man sein ganzes Leben profitieren. Die Herausforderung, auf sich alleine gestellt Problem zu meistern, lassen die Persönlichkeit wachsen und erweitern den Horizont. Erfahrungen in einem fremden Land sammeln, eine andere Sprache zu sprechen und neue Menschen und Kulturen kennen zu lernen ist eine wundervolle Sache. Unsere Studierenden besuchen ausgewählte Lehrveranstaltungen an der Partneruniversität, über ein Anrechnungssystem werden die absolvierten Kurse im aktuellen Studium anerkannt.

Sie haben mehr Bewerberinnen bzw. Bewerber als Studienplätze und der Andrang ist konstant hoch. Mit welchen Entwicklungen im IT-Security-Bereich rechnen Sie in Zukunft und gehen Sie davon aus, dass der Bedarf an Spezialistinnen bzw. Spezialisten im Bereich der IT bzw. Mobile-Security steigt? Welche Ideen haben Sie dabei für die Zukunft?

In Österreich fehlen aktuell etwa 30.000 IT Fachkräfte. Der Bedarf an hochqualifizierten Security Spezialisten wird weiterhin stark steigen. Unsere Absolventen haben durchgängig spannende, herausfordernde Jobs. Wir motivieren unsere Studierenden auch dazu, sich nach dem Studium selbstständig zu machen, dabei können wir bereits auf einige sehr erfolgreiche Beispiele verweisen. Gerade die IT-Security ist ein Themenfeld, wo lebenslanges Lernen notwendig ist. Täglich gibt es neue Sicherheitslücken, kreative Angriffsmethoden und die Anforderung, Systeme dagegen zu schützen. Ich hoffe, dass durch Investition in eine gute Ausbildung die Qualität und damit auch die Standfestigkeit von Systemen gegenüber der täglich steigenden Anzahl von Hackerangriffen steigen wird.

„In Österreich fehlen aktuell etwa 30.000 IT Fachkräfte. Der Bedarf an hochqualifizierten Security Spezialisten wird weiterhin stark steigen.“

IT & Mobile Security und IT-Recht & Management an der FH JOANNEUM

IT & MOBILE SECURITY UND IT-RECHT & MANAGEMENT AN DER FH JOANNEUM ABSOLVIEREN – NÄCHSTER SCHRITT PROMOTION?

Nach Ableistung des Grundwehrdienstes begann ich 2013 das Bachelorstudium Internettechnik an der FH JOANNEUM. Der Abschluss dieses Studiums schaffte ein solides Fundament für die Masterstudien IT & Mobile Security sowie IT-Recht & Management, welche ich 2015, respektive 2016 aufnahm. Diese Kombination deckt sowohl die technischen Sicherheitsaspekte als auch den rechtlichen und organisatorischen Rahmen der Informationssicherheit ab.

So konnte ich durch die Studienschwerpunkte Kryptographie, Software- und Netzwerk-Sicherheit sowie Computerstrafrecht, Datenschutzrecht und IT-Risikomanagement umfassende Kompetenzen in komplementären Themenfeldern aufbauen.
Das vermittelte theoretische Wissen wurde stets praktisch gefestigt: Beispielsweise wurden – neben mathematischer Beweise – kryptografische Verfahren, auch „hands-on" genannt, im Labor gelehrt; ebenso wurde unser Wissen zu Rechtsnormen mittels juristischer Sachverhalte in Übungsfällen geprüft. In beiden Studien erwies sich auch die umfassende Vorbereitung auf das wissenschaftliche Arbeiten als besonders nützlich. Ich habe an der Verbesserung der Sicherheit und Privatsphäre von Web-Analyse-Tools geforscht, wobei sich die erste Masterarbeit mit der technischen Sicherheitsanalyse befasste, und die zweite die datenschutzrechtlichen Anforderungen gemäß der DSGVO behandelte. Äußerst positiv in Erinnerung geblieben ist mir das Betreuungsverhältnis und die intensive Förderung von IT-Security-Talenten, etwa durch die Vorbereitung auf CTF-Wettbewerbe.

Die beiden Studien werden in berufsbegleitender Form angeboten und teilweise via Online-Lehre durchgeführt, sodass ich bereits während des Studiums wertvolle Berufserfahrung sammeln konnte. Seit 2017 bin ich nun Security-Forscher bei SBA Research sowie beim Christian Doppler Labor „SQI" und führe meine Spezialisierung im Rahmen eines Doktoratsstudiums an der TU Wien fort.

Matthias Eckhart, MSc MA

Security-Forscher
SBA Research

Zum Schluss

Danke für Ihr Interesse

Cyber-Security ist eine interdisziplinäre Querschnittsmaterie mit sehr komplexen Teilbereichen. Daher sind viele verschiedene Blickpunkte zu betrachten, um ein gesamtheitliches und vollständiges Bild über die Thematik zu bekommen.

Diese Broschüre gibt einen umfassenden Einblick in den Themenbereich Cyber-Security. Dazu wurden Beiträge von Universitäten, Fachhochschulen, Unternehmen und Organisationen sowie von Behörden und Institutionen zusammengetragen, da diese durch ihre Forschungsarbeit und Dienstleistungen ein aktuelles und reales Verständnis für Cyber-Security in den verschiedensten Bereichen haben.

Als Herausgeber dieser Broschüre wollen wir hiermit nochmals unseren herzlichsten Dank an alle ausrichten, die Materialien und Informationen für diese Broschüre bereitgestellt haben und dadurch zu diesem umfassenden Bild beigetragen haben. Vielen Dank!

Unser Dank gebührt aber ebenso den Leserinnen und Lesern dieser Broschüre für Ihr Interesse und wir hoffen Ihnen interessante Einblicke in die verschiedensten Themenbereiche und aktuellen Entwicklungen der Cyber-Security gegeben zu haben. Der A-SIT Guide ist somit ein wertvoller Beitrag zur Sensibilisierung und zur Wissensvermittlung sowie zum Erfahrungsaustausch.

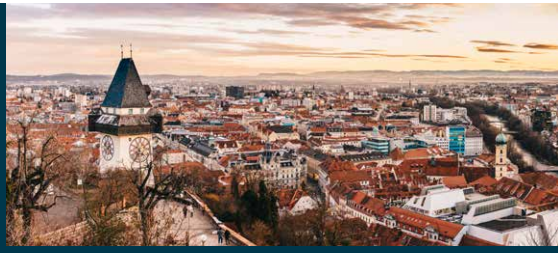
> „Damit Cyber-Security morgen genauso zuverlässig möglich ist wie bisher, bieten und realisieren wir bei A-SIT täglich Unterstützung in diesem Umfeld."

A-SIT

a-sit.at/

Ihr Partner für Sicherheitsfragen

A-SIT Zentrum für sichere Informationstechnologie – Austria



Büro Wien
Seidlgasse 22 I Top 9
1030 Wien I Österreich
E: office@a-sit.at
T: +43 1 503 19 63 - 0

Büro Graz
Inffeldgasse 16a
8010 Graz I Österreich
E: office@a-sit.at
T: +43 316 - 873 55 10

Entdecken Sie, wie A-SIT Ihnen bei der
Umsetzung von Cyber Security helfen kann:

a-sit.at/

„Wenn INVESTITIONEN
in CYBER-SECURITY erforderlich sind,
damit vorne,
morgen nicht gleich ganz hinten ist.“