Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

https://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

A-SIT, PARTNER IN FRAGEN DER IT-SICHERHEIT

IT-Sicherheit befasst sich mit dem Schutz elektronischer Daten und Dienste vor unberechtigtem Zugriff, Veränderung oder Missbrauch. Das ist eine notwendige Voraussetzung für den Einsatz der IT und schafft Vertrauen in neue Dienstleistungen wie etwa im E-Government. Öffentliche Institutionen sind heute nicht nur IT-AnwenderInnen, sondern zunehmend auch Anbieter von IT-basierten Dienstleistungen. Damit sind sie auch unmittelbar mit sämtlichen Aspekten und Problemen der IT-Sicherheit konfrontiert.

Hintergrund

Österreich hat das Thema elektronische Signaturen früh aufgegriffen und parallel zur EU-Richtlinie zu elektronischen Signaturen das Signaturgesetz erstellt. Zur Umsetzung musste rasch eine Aufsichts- und Bestätigungsinfrastruktur geschaffen werden. Dazu kamen bereits erste Überlegungen, im Zuge der Verwaltungsinnovation öffentliche Dienstleistungen auch elektronisch anzubieten. Parallel dazu entstand bei der Oesterreichischen Nationalbank im europäischen Kontext der Bedarf, den Risken der elektronischen Zahlungen zu begegnen: IT-Sicherheit wurde damit zu einem zentralen nationalen Thema.

Zugleich wurde der Bedarf nach einem kompetenten Ansprechpartner für befasste Behörden artikuliert. Eine solche Organisation sollte öffentlichen Institutionen nahe stehen und klare, kompakte Aussagen treffen können; etwa nach dem Vorbild des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Eine schlanke Organisation sollte gefunden werden, die sich effizient an die schnellen Veränderungen in der Informationstechnologie anpassen kann.

Im Mai 1999 wurde daher das Zentrum für sichere Informationstechnologie – Austria (A-SIT) vom Bundesministerium für Finanzen, der Oesterreichischen Nationalbank und der Technischen Universität Graz (TU Graz) gegründet. Mit Stand 2020 sind die Mitglieder von A-SIT das Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW für den Bund, Mitglied seit 2018), die Bundesrechenzentrum GmbH (BRZ GmbH, seit 2012), die TU Graz (Mitglied seit 1999) und die die Donau Universität Krems (DUK, seit 2018).

Zwecks raschester Umsetzung wurde die Rechtsform eines Vereines aus institutionellen Mitgliedern gewählt. Für die Aufgabenstellung waren und sind festgeschriebene, aber auch gelebte Weisungsfreiheit und Neutralität unabdingbar. Bewusst wurde kein Amt gegründet, sondern ein Rahmen für unbürokratische, flexible sowie kostengünstige Gebarung geschaffen – dies hat sich bis heute bewährt.

Im Juli 2015 wurde die A-SIT Plus GmbH gegründet, die Leistungen zur technischen Informationssicherheit sowohl öffentlichen, wie auch privatwirtschaftlichen Organisationen anbietet.

A-SITs Aktivitäten decken vor allem drei große Ebenen der IT-Sicherheit ab:

- Bestätigung / Begutachtung / Evaluierung
- Forschung und Technologiebeobachtung
- innovative Anwendungsunterstützung auf hohem Niveau

Weiters wird ein Beitrag zur Stärkung des IT-Sicherheitsbewusstseins im Allgemeinen geleistet.

Nicht zuletzt hat die wirtschaftliche Entwicklung der letzten Zeit gezeigt, dass Aufsicht über komplexe Prozesse, Beobachtung von Entwicklungen und Innovationen wünschenswerte Mittel zur Stärkung der Volkswirtschaft sind.

Tätigkeitsbereiche:

Bestätigungsstelle nach § 7 Signatur- und Vertrauensdienstegesetz

Bei den elektronischen Signaturen sehen die seit Juli 2016 geltende eIDAS Verordnung[1] und das Signatur- und Vertrauensdienstegesetz einen offenen Marktzugang ohne behördliche Genehmigung vor. Qualifizierte elektronische Signaturen sind der Schriftform gleichgestellt und stellen daher hohe Ansprüche an die technische Sicherheit. Diese wird durch eine Infrastruktur gewährleistet, bestehend aus Aufsichtsstelle (Telekom Control Kommission; TKK), Bestätigungsstelle und akkreditierten Konformitätsbewertungsstellen. Es ist die Aufgabe der Bestätigungsstelle, die Sicherheit besonders sensibler technischer Komponenten für elektronische Signaturen zu überprüfen und zu bescheinigen. Ein detaillierter Prüfbericht macht das korrekte Zustandekommen der Bescheinigung nachvollziehbar. Dies erfordert ein besonders hohes Maß an technischer Qualifikation, Erfahrung, Exaktheit und Korrektheit. A-SITs Eignung als Bestätigungsstelle wurde durch Verordnung des Bundeskanzlers vom 2. Februar 2000 (nach dem bis 30.6.2016 gültigen Signaturgesetz) bzw. vom 1. August 2016 (nach dem ab 1.7.2016 gültigen Signatur- und Vertrauensdienstegesetz) festgestellt.

Qualifizierte elektronische Signaturen sind eine Basistechnologie für E-Government, wurden aber auch bei den Hochschülerschaftswahlen (e-voting) eingesetzt.

Akkreditierte Konformitätsbewertungsstelle

Seit Dezember 2016 ist A-SIT als Produktzertifizierungsstelle gemäß EN ISO/IEC 17065:2012 akkreditiert. Der Akkreditierungsumfang umfasst dabei die in der eIDAS Verordnung vorgesehenen Tätigkeiten für Konformitätsbewertungsstellen.
Hauptaufgabe der Konformitätsbewertungsstelle des Vereins A-SIT ist es, Vertrauensdiensteanbieter an Hand der Anforderungen der eIDAS Verordnung und darauf basierender europäischer Normen zu überprüfen. Als Ergebnis werden Konformitätsbewertungsberichte ausgestellt, die von den Vertrauensdiensteanbietern der zuständigen Aufsichtsstelle vorgelegt werden müssen. Die Durchführung der Konformitätsbewertungen muss anhand der durch die internationale Norm EN ISO/IEC 17065 vorgegebenen Qualitätssicherungsmaßnahmen erfolgen, das eigene Qualitätsmanagement der Konformitätsbewertungsstelle hat daher einen dementsprechend hohen Stellenwert.

Seit der Akkreditierung als Konformitätsbewertungsstelle wird A-SIT laufend von Vertrauensdiensteanbietern für deren wiederkehrend notwendige Bewertungen herangezogen.

Gutachterliche Tätigkeit

Für Überprüfungen bzw. Aussagen über IT-Sicherheit, welche nicht unter die zuvor beschriebenen formalen Schemata fallen, hat A-SIT die Funktion eines Amts- bzw. Privatgutachters. Als Amtsgutachter ist A-SIT im Auftrag der Datenschutzbehörde tätig, ansonsten werden hauptsächlich von öffentlichen Institutionen Sicherheitsgutachten zu klaren Fragestellungen beauftragt.

Beispiele sind technische Aussagen im Zuge von Beschwerden bei der Datenschutzbehörde resp. Prüfaussagen über Signatur-Komponenten, die nicht unter die Bestätigungspflicht fallen, im Auftrag der Aufsichtsstelle.

Bürgerkarte, E-ID und E-Government

E-Government in seiner Gesamtheit stellt eine der bedeutendsten Innovationen in der öffentlichen Verwaltung dar: Der Wegfall des Papieraktes machte die Verwaltungstätigkeit unabhängig von Zeit und Ort. In der elektronischen Kommunikation mit bzw. innerhalb der öffentlichen Verwaltung ist IT-Sicherheit von besonderer Bedeutung. Nur die berechtigte Person darf ein Verfahren anstoßen, einen Bescheid elektronisch zugestellt bekommen resp. einen elektronischen Akt bearbeiten. Im elektronischen Verfahren kann die Bürgerkarte (bzw. nach Umsetzung der Novelle E-Government Gesetz 2017 der „E-ID“) den Benutzer/die Benutzerin identifizieren (Äquivalent zum Ausweis) und seine/ihre elektronische Signatur auslösen (Äquivalent zur Unterschrift).

Damit kann je nach Rolle der Benutzer bzw. Benutzerinnen das komplette Verfahren elektronisch abgebildet werden: Vom Anbringen (Antrag) des Bürgers/der Bürgerin über Zugangserlaubnis der Bearbeiter bzw. Bearbeiterinnen bis zur elektronischen Zustellung.

[1] Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Das von A-SIT verfasste „Weißbuch Bürgerkarte“ stellte die grundlegenden Konzepte im Zusammenhang mit Bürgerkarten zusammen. Im nächsten Schritt wurden von A-SIT, in Zusammenarbeit mit der Plattform Digitales Österreich, Spezifikationen erstellt, Konzepte abgestimmt und Referenzimplementierungen (Proof of Concept) umgesetzt. Dabei entwickelte Prototypen wurden als Referenz frei zur Verfügung gestellt.

Prototypen oder Tools zur Nutzung der Bürgerkarte und des E-ID werden weiter entwickelt und kostenfrei allen Interessierten zur Verfügung gestellt, z.B. „PDF-OVER“ (PDF Signatur mit Bürgerkarte) oder „Citizen Card Encrypted – CCE“ (Datenverschlüsselung mittels Bürgerkarte).

Eine erfolgreiche Entwicklung in Richtung Vereinfachung stellt die „Handy-Signatur“ dar, welche unabhängig von Karten, Lesern bzw. dezidierten PC’s bei höchster Sicherheit funktioniert.

A-SIT brachte sein Wissen und seine Erfahrung im Rahmen der europäischen Large Scale Pilots STORK und STORK 2.0 (wechselseitige Anerkennung nationaler elektronischer Identitäten) und epSOS (europaweite Gesundheitsdaten (Patient Summary) sowie elektronische Rezepte) ein. Beide basieren auf einer sicheren elektronischen Identitätsfeststellung, wie sie in Österreich die Bürgerkarte und ab 2020 der neue E-ID bietet. Dies wurde im Large Scale Pilot eSENS weitergeführt, der die Basiskomponenten der vorigen Large Scale Pilots konsolidiert.

A-SIT unterstützt das Bundesministerium für Digitalisierung und Wirtschaftsstandort in den Expertengruppen und dem Kooperationsnetzwerk zur EU eIDAS Verordnung.

Forschung und Technologiebeobachtung

Voraussetzung für die Erhaltung der Kompetenz ist die laufend aktuelle Kenntnis des Standes von Technik, Wissenschaft und praktischen Erfahrungen in der Informationssicherheit. Dazu gehören die Eigenschaften sicherheitstechnisch relevanter Systeme und Produkte sowie die laufende Analyse erreichbarer Sicherheitsniveaus und möglicher Risiken. In Forschung und Technologiebeobachtung befasst sich A-SIT daher u.a. mit der Analyse kryptographischer Verfahren und von Signaturalgorithmen zur Bestimmung ihrer Robustheit gegen Angriffe (z.B. Seitenkanalattacken (DPA, SPA) auf Chipkarten).

Zur Tätigkeit gehören internationale Forschungsprojekte bzw. die aktive Mitwirkung in internationalen Normungsgremien. Über wissenschaftliche Berichte und Stellungnahmen hinaus entstehen wichtige Normen – etwa technische Standards zur Umsetzung der EU-Signaturrichtlinie, etwa mit ETSI und zuvor im Rahmen der European Electronic Signature Standardisation Initiative (EESSI).

Zunehmende Bedeutung erlangt der Schutz kritischer Infrastrukturen, welche schon jetzt vom Funktionieren ihrer IT-Systeme abhängen. Die Bedrohung liegt einerseits im Ausfall oder Kontrollverlust vitaler Einrichtungen (z.B. Stromversorgung, Zahlungsverkehr,...) aber auch im Auftreten zwar begrenzter, aber nicht erklärbarer Vorfälle mit hoher Öffentlichkeitswirkung (z.B. Fehler im Gesundheitswesen oder in der Verwaltung).

A-SIT ist zwar kein operativer Player der österreichischen govCERT-Struktur, hat allerdings zu ihrer Entstehung beigetragen. Am Beginn stand 2008 ein hochrangiger internationaler Erfahrungsaustausch anlässlich der Fußball-EM, danach die Mitwirkung beim Initiieren des govCERT.

Aktuelle Schwerpunkte der Forschung und Technologiebeobachtung sind – neben den laufend bearbeiteten Kernthemen Kryptographie, elektronische Signatur und elektronische Identität – nicht zuletzt aus dem Bedarf in der Verwaltung die Sicherheit von und Mobiltechnologien und Cloud Computing.

Unterstützung von Institutionen

A-SIT stellt eine Ansprech- und Koordinierungsstelle für IT-Sicherheit dar. Die Fragestellungen sind vielfältig und reichen von einfachen Anfragen bis zu umfassenden Gesamtaussagen bei Großvorhaben.

Öffentliche Stellen nutzen die Kompetenz von A-SIT, wenn etwa neue Regulative mit technischen Inhalten zu erstellen, sicherheitsrelevante Konzepte zu schaffen oder Konformitätsaussagen – etwa Verträglichkeit eines Implementierungsvorhabens mit den E-Government Spezifikationen – zu treffen sind. Dabei hat sich die weisungsfreie und interessensneutrale Unterstützung durch A-SIT bewährt.

Darüber hinaus konnte bei A-SIT durch die jahrzehntelange Kooperation mit der Oesterreichischen Nationalbank (OeNB) als zuständige Aufsichtsbehörde im Umfeld der Zahlungssystemaufsicht (ZSA) eine starke Expertise zum Thema Zahlungssysteme aufgebaut werden.

Dazu werden auch allgemeingültige Empfehlungen für die Informationssicherheit in Organisationen erstellt.

Bekanntes Beispiel ist das Österreichische Informationssicherheitshandbuch, das laufend aktualisiert wird.

Internationales

Wesentlich ist die internationale Zusammenarbeit, vor allem mit vergleichbaren Organisationen im europäischen Raum. Dazu wurden Kooperationsvereinbarungen mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Schweizer Informatiksteuerungsorgan des Bundes (ISB) und Deutschland sicher im Netz (DsIN) geschlossen. Dies wurde im deutschsprachigen Raum um Kooperation mit der luxemburgischen Agence nationale de la sécurité des systèmes d'information (ANSSI) ergänzt.

Die Mitgliedschaft und Teilnahme in international koordinierenden Gremien (z.B. ENISA, Common Criteria, SOG-IS, OECD, …) optimiert das Fachwissen von A-SIT sowohl auf dem Gebiet der technischen Normung, als auch bei der Umsetzung technischer Verfahren. Beim Mitwirken an EU-Projekten wird die Kompetenz von A-SIT immer wieder unter Beweis gestellt.

Aus der internationalen Vernetzung kann A-SIT Vorhaben anderer Länder beobachten und bei aktuellen Entwicklungen zu koordiniertem Vorgehen beitragen.

Awareness

Der Einsatz von sicherer Informationstechnik in Wirtschaft und Verwaltung in breitem Anwendungsspektrum benötigt das Vertrauen der Benutzer und Benutzerinnen. Sie können das tatsächliche Sicherheitsniveau nicht nachprüfen. Sicherheitsmaßnahmen sollen auch nicht als Behinderung im Arbeitsalltag, sondern als notwendiger Schutz empfunden werden.

Es gehört zur Erwartung an A-SIT zur Bewusstseinsbildung beizutragen. Elektronische Informationsschiene ist die Homepage www.a-sit.at, die sich vor allem an interessiertes Fachpublikum richtet. Mit der Betreuung des IKT-Sicherheitsportals www.onlinesicherheit.gv.at werden von Laien bis hin zu Profis alle über Gefahren und Entwicklungen im IT-Bereich informiert sowie das Bewusstsein der Bevölkerung hinsichtlich Cyberrisiken gestärkt. Als weiterer Informationsschwerpunkt werden Awareness-Veranstaltungen durchgeführt, die sich an Entscheidungsträger und Entscheidungsträgerinnen sowie Spezialisten und Spezialistinnen aus Wirtschaft und öffentlicher Verwaltung wenden.

Öffentliche Auftritte wurden bisher – schon wegen der Kosten – eher vermieden, vielmehr wird Organisationen kompaktes Wissen und Argumentarium für öffentliche Aussagen übermittelt.

Aus der zielgruppenorientierten Aufbereitung technischer Zusammenhänge verbreitet A-SIT Expertenwissen an Fachkreise, richtet sich in Kooperation mit Partnern auch an breiteres Publikum, wie Informationen über www.buergekarte.at oder www.onlinesicherheit.gv.at.

Organisatorische Aspekte:

Das Zentrum für sichere Informationstechnologie Austria (A-SIT) ist nach wie vor ein gemeinnütziger Verein aus den institutionellen Mitgliedern BMDW, TU Graz, BRZ GmbH und DUK. Unter der Leitung der beiden Vorstände sind zurzeit 8 Mitarbeiter und Mitarbeiterinnen fix angestellt und bis zu 10 Personen über den Ressourcenpool der TU Graz tätig.

Die Gebarung wird sowohl inhaltlich wie wirtschaftlich von mehreren Kontrollinstanzen geprüft: Beginnend mit seinen eigenen statutarischen Organen (Präsidium, Rechnungsprüfung, Generalversammlung) findet jährlich eine Wirtschaftsprüfung statt.

Die A-SIT Plus GmbH steht im 100%-igen Eigentum des Vereins A-SIT und kann Leistungen zur technischen Informationssicherheit sowohl öffentlichen wie auch privatwirtschaftlichen Organisationen anbieten und ist so am Markt tätig.

Assets und Perspektiven

Mit der Gründung von A-SIT wurde seinerzeit Neuland beschritten. In mittlerweile über 20 Jahren wurden im Rahmen der Größe und Möglichkeiten anerkannte Erfolge erzielt und Erfahrungen gewonnen. Der Bereich Bestätigungsstelle wird ein notwendiges öffentliches Service für einen hoch spezialisierten Teil der IT-Industrie bleiben. Damit wird eine dem kleinen österreichischen Markt angemessene Infrastruktur für anerkannte System- und Produktevaluierungen geboten.

Die Technologiebeobachtung greift technische Trends frühzeitig auf und behandelt schwerpunktmäßig vor allem jene Themen der IT-Sicherheit, an denen öffentliches Interesse besteht, Auswirkungen auf die Allgemeinheit zu erwarten sind oder Synergien zu anderen Tätigkeitsbereichen von A-SIT bestehen.

Bei der Unterstützung öffentlicher Institutionen ist künftig steigender Bedarf – von öffentlichen Stellen wie aus der Wirtschaft – an sicherheitstechnischer Begleitung zu erwarten, nachdem die Konzepte nun zusehends europaweit umgesetzt werden. Die EU-Dienstleistungsrichtlinie zwingt alle Gebietskörperschaften zum Angebot sicherer elektronischer Kommunikation mit den Bürgern und Bürgerinnen, dies wird die EU Verordnung zur Einrichtung eines einheitlichen digitalen Zugangstors noch erweitern.

Damit die elektronischen Verfahren Akzeptanz finden und somit auch angewendet werden, muss Bewusstsein gebildet und kompakte Information gegeben werden. Dann wird der angestrebte Erfolg – Vereinfachung, Beschleunigung und letztlich Kosteneinsparung – erreicht.

A-SIT ist unbeschadet des Bekenntnisses zur internationalen Zusammenarbeit eine österreichische Einrichtung und will weiterhin einen Beitrag zur Stärkung des Technologiestandorts Österreich leisten.

AnsprechpartnerInnen:

Geschäftsführung A-SIT Verein:

Gesamtleiter: o. Univ. Prof. Dr. Reinhard Posch reinhard.posch@a-sit.at
Generalsekretär: Dipl.-Ing. Herbert Leitold herbert.leitold@a-sit.at

Bereich Inspektion, Zahlungssysteme, Bestätigung, Awareness (IZBA)

Bereichsleiter: Dipl.-Ing Dipl.-Ing Gerald Dißauer gerald.dissauer@a-sit.at

Bereich Technologie und E-Government (TGV)

Bereichsleiter: Dipl.-Ing Herbert Leitold herbert.leitold@a-sit.at

Geschäftsführung A-SIT Plus GmbH:

Geschäftsführer: Dr. Peter Teufl peter.teufl@a-sit.at