CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE OF TECHNOLOGY

CAIS – CYBER ATTACK INFORMATION SYSTEM

Intelligente Cyber Security Lösungen für den Schutz industrieller Steuerungssysteme

THE TIMES THEY ARE CHANGING

Vorwort von Helmut Leopold, Head of Center for Digital Safety & Security,
AIT Austrian Institute of Technology.

In unserer modernen, global vernetzten und durch Digitalisierung bestimmten Gesellschaft haben sich die Spielregeln zur Beherrschung der digitalen Technik zum Wohle der positiven gesellschaftlichen und wirtschaftlichen Entwicklung grundlegend verändert. Zum einen bauen wir durch die umfassende Vernetzung in all unseren Lebensbereichen komplexe Systeme, welche sich nicht mehr einfach deterministisch verhalten. System of Systems, Internet of Things (IoT) und Cyber Physical Systems bezeichnen die zunehmende Komplexität unserer technischen Plattformen, welche es immer schwieriger macht, die Systeme im Detail sowie vollständig zu verstehen und starre Regeln zu definieren, um korrektes Systemverhalten zu beschreiben.

Aus wirtschaftlichen Gründen und aus fehlendem Bewusstsein von Kunden, wirtschaftlichen Akteuren und der breiten Gesellschaft hat sich – im globalen Kontext – keine umfassende Sicherheitskultur entwickelt. Aus Sicht des Betriebes von Technik gehen wir alle sehr nachlässig mit Passwörtern und elektronischem Zugriffsschutz um. Hersteller von technischen Geräten für alle Industriebereiche wie beispielsweise für moderne Fahrzeuge, Produktionssteuerungsanlagen (Industrielle Steuerungssysteme), Energienetze, Smart Homes, etc. bauen Sicherheitsmechanismen noch nicht umfassend bereits im Zuge ihrer Entwicklungsprozesse mit ein.

Diese fortlaufende Digitalisierung führt zu einer immer höheren Abhängigkeit von technischen Systemen und zu einem stetig ansteigenden Risiko bei deren Verwendung. Gleichzeitig haben sich das Ausmaß und die Professionalität der Bedrohungen in den letzten Jahren wesentlich verändert. Während zu Beginn das Interesse an der Technik im Vordergrund stand und die ersten Viren ohne kommerziellen Fokus entwickelt wurden, haben in den letzten Jahren politische und wirtschaftliche Interessen als Motivationsfaktoren eine führende Rolle eingenommen. Die Bedrohung geht nicht mehr von einzelnen, isoliert arbeitenden Hackern aus, sondern von organisierten Strukturen mit beträchtlichen Investitionen in entsprechende Angriffe.

Diese massive Entwicklung hat sich erst in den letzten Jahren zu diesem Ausmaß zugespitzt und stellt die Industrie, aber auch die Gesellschaft vor neue Herausforderungen im Umgang mit der Cyber-Domäne. Um diese bewältigen zu können, braucht es ein umfassendes Bewusstsein aller Entscheidungsträger und auch aller Kunden darüber, dass sichere Systeme nicht nur ein Kostenfaktor sind, sondern eine unbedingte Notwendigkeit, eine gemeinsame sichere, globale Infrastruktur für unsere digitale Gesellschaft zu bauen und unsere Privatsphäre umfassend zu schützen.

INTELLIGENTE CYBER SECURITY LÖSUNGEN MADE IN AUSTRIA

All dies macht eine umfassende gemeinsame Forschungsanstrengung notwendig, um unsere technischen Systeme widerstandsfähiger gegenüber Ausfällen und feindlichen Zugriffen zu machen. Wir müssen viel besser verstehen lernen, in welcher Weise unsere gesellschaftlichen Prozesse von einzelnen technischen Systemen abhängen, um geeignete Maßnahmen in einem ökonomischen und gesellschaftlichen Kontext zu setzen.

In Österreich gibt es in verschiedensten Bereichen SpitzenforscherInnen und auch global führendes Know-how. Im Cyber Security Kontext verfolgen wir am AIT in der Technologieentwicklung, die sich vor allem auf den Schutz von kritischen Infrastrukturen und industriellen Steuerungssystemen konzentriert, folgende Schwerpunkte: spezielle Systemdesigns für widerstandsfähige industrielle Steuerungssysteme und kritische Infrastrukturen (Security by Design); neuartige Verfahren der intelligenten Datenverschlüsselung (Smart Encryption) in Internet of Things-(IoT) sowie Cloud-Systemen für höchstmögliche Datensicherheit und den Schutz der Privatsphäre; ein revolutionäres Immunsystem für technische Systeme in Form einer intelligenten und lernfähigen Software (Machine Learning), die selbst die gefinkeltsten Cyber-Attacken erkennt; und schließlich fokussieren wir uns auf entsprechende Cyber Test- und Ausbildungsplattformen (Cyber Range), um den Aufbau von speziellen Fähigkeiten für Entwickler und Betreiber von IT-Systemen zu unterstützen.

EUROPÄISCHER VORREITER IM BEREICH CYBER SECURITY

Dank des speziellen Know-hows am AIT gilt Österreich international als Hightech-Standort für Cyber Security. Aufgrund seiner langjährigen Erfahrung im Bereich digitaler Sicherheit hat sich das AIT auf diesem Gebiet als verantwortungsvoller Partner für die entsprechenden nationalen Behörden und als anerkannte Institution für Cyber Security in der europäischen Forschungslandschaft etabliert. Die ExpertInnen des AIT setzen auf Machine Learning, um bahnbrechende Technologien und Lösungen für das künftige Cyber Security Ökosystem zu entwickeln und damit den Bedrohungen entgegenzuwirken, die sich durch neue umfangreiche IKT-Infrastrukturen mit steigender Vernetzung und unklaren Angriffsflächen ergeben. Diese speziellen IT-Sicherheitslösungen setzen neue Standards und tragen dazu bei, die Wettbewerbsfähigkeit heimischer Produkte auf dem globalen Markt durch österreichisches Know-how sicherzustellen.

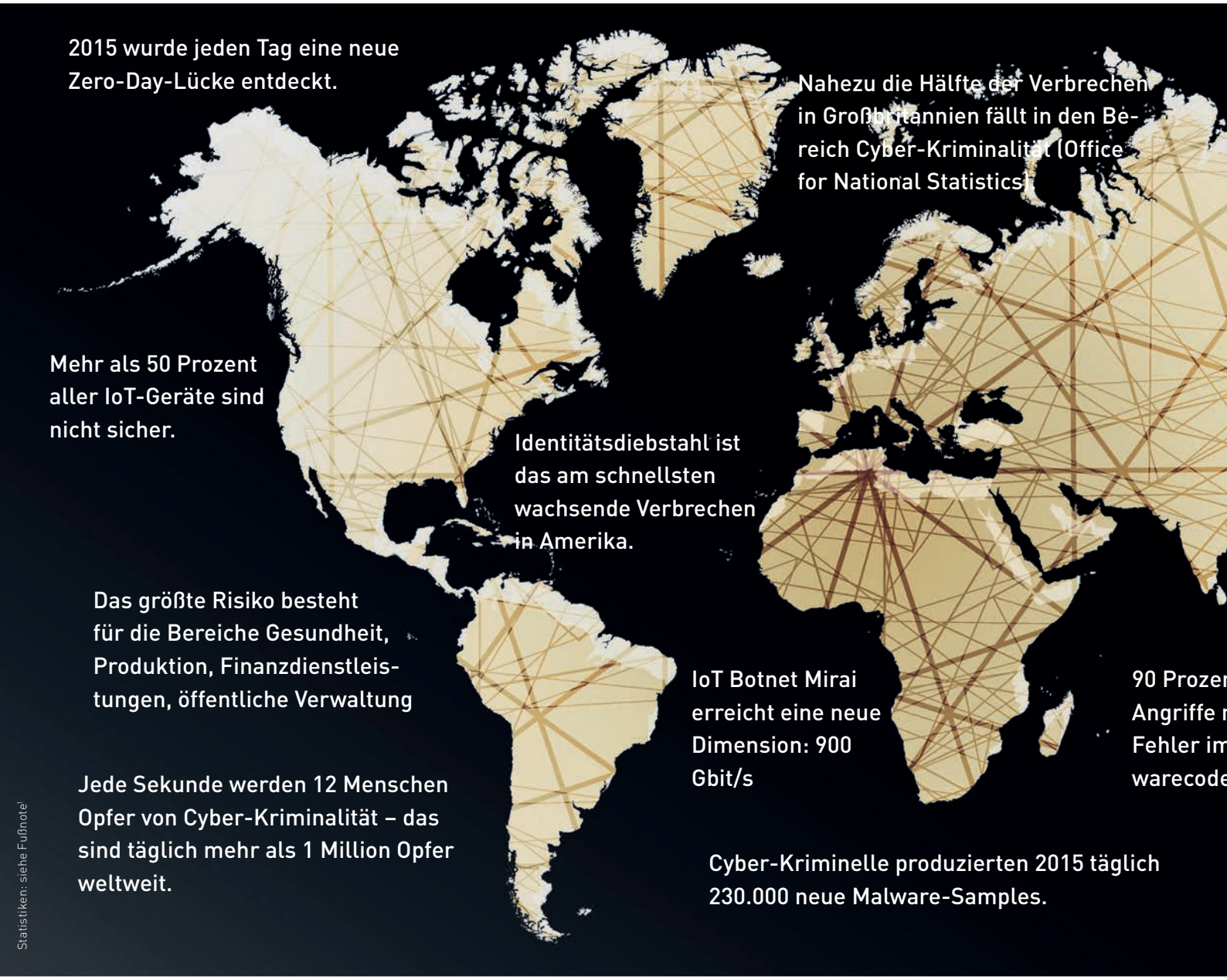
MACHINE LEARNING ERHÖHT DIE WIDERSTANDSFÄHIGKEIT VON KOMPLEXEN DIGITALEN SYSTEMEN

Die steigende Komplexität unserer IT-Systeme erfordert neue Mechanismen, um sie vor ausgeklügelten Cyber-Attacken zu schützen, Anomalien im komplexen Systembetrieb zu entdecken oder fehlerhafte Bedienung durch die IT-User selbst zu erkennen. Drei Elemente sind beim Aufbau der resilienten digitalen IT-Systeme der Zukunft erforderlich: neuartige Risikomanagementlösungen auf Basis klar definierter Bedrohungskataloge, die Harmonisierung der Sicherheitsmethoden (Safety & Security Co-Design) sowie Echtzeit-Monitoring von IT-Systemen zur Anomalieerkennung mit Hilfe neuartiger Machine Learning Konzepte.

Helmut Leopold, Head of Center for Digital Safety & Security, AIT

Indem wir unsere digitalen Systeme mit künstlicher Intelligenz ausstatten, erhöhen wir ihre Widerstandsfähigkeit gegen Einflüsse, die unsere IT-Systeme destabilisieren könnten.

INHALTSVERZEICHNIS



Statistiken: siehe Fußnote!

DER GLOBALE CYBER-BEDROHUNGSMARKT

Eine Bestandsaufnahme des weltweiten Markts für Cyber-Kriminalität.

Um ein klareres Bild der Cyber-Bedrohungen zu erhalten, müssen wir das Phänomen aus zwei verschiedenen Blickwinkeln betrachten. Die weltweiten Ausgaben für Produkte und Dienstleistungen im Bereich Cyber Security werden laut Schätzungen von Cybersecurity Ventures im Zeitraum von 2017 bis 2021 mehr als 1 Billion US Dollar betragen. Diese Prognosen scheinen mit den Cyber-Bedrohungen jedoch nicht Schritt halten zu können. Dazu zählen der dramatische Anstieg der Cyber-Kriminalität, die rasend schnelle Ausbreitung von Ransomware, die Verlagerung von Schadprogrammen von PCs und Laptops auf Smartphones und mobile Geräte, der Einsatz von Milliarden unzureichend geschützter Geräte im Internet of Things (IoT), die Legionen von bezahlten Hackern sowie die immer ausgeklügelteren Cyber-Attacken auf Unternehmen, Regierungen, Bildungseinrichtungen und Konsumenten weltweit.

Schätzungen zufolge werden die jährlichen weltweiten Kosten für Cyber-Kriminalität von 3 Billionen US Dollar 2015 auf 6 Billionen US Dollar 2021 ansteigen. Dazu zählen Faktoren wie die Beschädigung und Zerstörung von Daten, Gelddiebstahl, Produktivitätsverlust, Diebstahl von geistigem Eigentum, Diebstahl von personenbezogenen und Finanzdaten, Unterschlagung, Betrug, Störung der normalen Geschäftstätigkeit, forensische Untersuchungen, Wiederherstellung und Löschung gehackter Daten und Systeme bis hin zu Rufschädigung, um nur einige zu nennen. Unsere vernetzte Welt wird auch zu einem massiven Anstieg im Datenvolumen führen und damit eine größere Angriffsfläche für Cyber-Attacken bieten. Internationalen Schätzungen zufolge wird die zu schützende Datenmenge in den kommenden fünf Jahren um das 50-fache ansteigen. Darüber hinaus wird das Internet of Things (IoT) mit neuen elektronischen Geräten in Unterhaltungselektronik,

Wearables, medizinischen Anwendungen, Industrie 4.0, Fahrzeugen, öffentlicher Sicherheit und Umwelt künftig neue Einfallsrouten für Kriminelle eröffnen.[1]

Der Schwarzmarkt im Untergrund wächst ständig. Die Cybercrime-Foren haben sich zu professionellen Plattformen entwickelt, die von gut organisierten kriminellen Unternehmen und sogar einigen Nationalstaaten genutzt werden. Das Insiderwissen zur Durchführung gewinnbringender Attacken hat sich seit den ad hoc organisierten Gruppen der Vergangenheit vervielfacht und dient nicht mehr allein der Befriedigung des Bedürfnisses nach Ruhm und Selbstbestätigung.

Die heutigen Schwarz- und Grau-Märkte sind Erweiterungen des organisierten Verbrechens im Cyberspace und haben sich in den vergangenen Jahren signifikant weiterentwickelt. Mit anderen Worten: rund 20% der professionellen Kriminellen haben sich Spezialwissen angeeignet und üben ihr zerstörerisches Werk nun mit Hilfe intelligenter und hochmoderner Technologien aus. Mit der Möglichkeit zum Diebstahl intelligenter IT-Tools hat sich das Leistungsangebot ausgeweitet und reicht nun vom Verkauf gestohlener Kreditkarten, Bankkonten, IP- und E-Mail-Adressen bis hin zu Phishing- und Spam-Attacken, bezahlten DDoS-Angriffen und einfach zu bedienenden Botnets.

Jeder mit genügend krimineller Energie kann heutzutage das erforderliche Waffenarsenal im Darknet kostengünstig von Agenten anmieten und damit unterschiedliche Attacken ausführen. Das gefährlichste an der neuen Cybercrime-Welt ist jedoch, dass man als Verbrecher nicht einmal selbst auf dem Gebiet versiert sein muss. Wem das cyberkriminelle Talent fehlt, kann andere für die Aufgaben anheuern, wenn das Geld stimmt.

Darüber hinaus können kriminelle Neulinge selbst leicht Opfer von erfahreneren Verbrechern werden, die ihnen zum Beispiel zuerst 10 gültige Kreditkarten gratis überlassen, um ihnen dann tausende abgelaufene oder ungültige Karten zu verkaufen, wie eine RAND-Studie[2] berichtet.

Die Vorhersagen für die künftigen Entwicklungen im Bereich Cybercrime sind daher pessimistisch:

- Steigende Aktivität in Darknets, genauere Überprüfung der Teilnehmer, stärkere Nutzung von Kryptowährungen, größere Anonymität bei Malware und stärkere Verschlüsselung und Schutz von Kommunikation und Transaktionen.
- Unterstützt durch solche Märkte wird das Angriffspotenzial die Verteidigungsfähigkeit bald übersteigen.
- Hyperconnectivity wird mehr Angriffspunkte für Verbrechen mit stärkerer Netz- und Cyberkomponente bieten und damit auch mehr Möglichkeiten für Schwarzmärkte eröffnen.
- Die Nutzung sozialer Netzwerke und mobiler Endgeräte wird weiter ansteigen.
- Es wird mehr Miet-Hacker, "As-a-Service"-Angebote und Zwischenhändler geben[2]

Die gesamte Cyber Security Industrie ist dringend gefordert, in den kommenden Jahren ihre stärksten Verteidigungswaffen gegen die Cybercrime-Szene aufzubieten und die technologische Reife und Intelligenz ihrer Systeme zu stärken.

[1] "Hackerpocalypse: A Cybercrime Revelation", Steve Morgan, Editor-in-Chief, Cybersecurity Ventures; A 2016 report from Cybersecurity Ventures sponsored by Herjavec Group, Q3 2016; http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, page 6

[2] RAND, National Security Research Division; Lillian Ablon, Martin C. Libicki, Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data Hackers' Bazaar", Sponsored by Juniper Networks, 2014)

ADVANCED PERSISTENT THREATS (APT)

Wie Advanced Persistent Threats definiert und ausgeführt werden.

In den vergangenen Jahren hat die "Black Hat" Community eine Vielzahl profitabler Konzepte zum Identitätsraub entwickelt und damit enorme Mengen personenbezogener Daten aus dem unternehmerischen und behördlichen Sektor abgesaugt. Disruptive Änderungen der IT-Infrastruktur sowie neue Nutzungsmodelle wie Mobilität, Cloud Computing und Virtualisierung haben die traditionellen Sicherheitszonen der Unternehmen aufgelöst und den Weg zu ergiebigen Datenumgebungen geebnet. Diese werden nun durch internationale Spionage- und Sabotagekampagnen angegriffen, um unter Mithilfe von Akteuren aus dem Umfeld der organisierten Cyberkriminalität geistiges Eigentum (IP) zu stehlen.

Solche gezielten Attacken werden auch als APTs (Advanced Persistent Threat, dt. "fortgeschrittene, andauernde Bedrohung") bezeichnet. „Advanced" bedeutet, dass die kriminellen Akteure das gesamte technologische Spektrum unerlaubter Computerzugriffe (z.B. Drive-by Downloads, SQL Injection, Malware, Spyware, Phishing und Spam) ausnutzen und mit Techniken des Social Engineering verknüpfen. Bei Bedarf verbessern sie ihre Zugriffstools weit über den Level der allgemein erhältlichen Selbstbausätze und Standardprodukte hinaus. Mit Hilfe von „Kill Chains", wie Exploits für Zero-Day-Lücken, Viren, Würmer und Rootkits, suchen die Angreifer unter Umgehung der eingerichteten Verteidigungsbereiche ihren Weg durch das gekaperte Netzwerk, um „vertrauenswürdige Verbindungen" für ihre Zwecke zu missbrauchen. Dafür werden Verschlüsselungen geknackt, um sich so als normaler Netzwerkverkehr zu tarnen.

„Persistent" bedeutet, dass die Angreifer sich auf eine Aufgabe und ein Ziel konzentrieren, wobei sie in den meisten Fällen durch externe Organisationen gesteuert werden. APTs erfolgen schleichend und in kleinen Schritten und basieren auf laufender Überwachung und Interaktion, um die definierten Ziele zu erreichen und über längere Zeit hinweg unentdeckt zu bleiben.

Im nächsten Schritt sammeln APTs zielgerichtet geheime Daten und vertrauliche Informationen wie etwa Betriebs- oder Militärgeheimnisse. Es handelt sich dabei üblicherweise um äußerst anspruchsvolle Angriffsszenarien, die eine volle Fernsteuerbarkeit der angegriffenen Informationsinfrastruktur zum Ziel haben.

Regierungsbehörden, Hersteller von Produkten, die auf dem globalen Markt einem großen Wettbewerb ausgesetzt sind und Betreiber von kritischen Infrastrukturen wie Energieunternehmen, Kraftwerke, Regierungseinrichtungen oder große Datenbanken haben daher das höchste Risiko, Opfer eines ernsthaften und von langer Hand geplanten APTs zu werden.

WAS IST MACHINE LEARNING?

Im weiteren Sinn bezeichnet Machine Learning eine Reihe von Techniken, mit deren Hilfe Maschinen lernen, selbständig Probleme zu lösen. Im ersten Schritt des Machine Learning Prozesses wird die Maschine mit Informationen über Ausprägungen oder typische Muster eines für die Informationsverarbeitung wichtigen Aspekts gefüttert. Sobald die Maschine ihre Lektionen durch ständige Wiederholung der trainierten Erkennungsroutinen (Machine Learning Modell) mit Hilfe von Analysealgorithmen gelernt hat, kann sie ihre Wirksamkeit durch immer genauere Vorhersagen der Zukunft verbessern.

Der rasante Aufstieg von Data Science, landläufig als Big Data bezeichnet, und die reichliche Verfügbarkeit von kostengünstiger Rechenleistung zur Speicherung, Übertragung und Auswertung von Datensätzen hat das Machine Learning in den letzten Jahren beflügelt. Derzeit sind in der Cyber Security Industrie zwei Trends zu bemerken, die zu noch leistungsfähigeren Machine Learning Technologien führen werden: zum einen werden tagtäglich große Mengen von Rohdaten gesammelt und ist bereits eine Vielzahl von IT-Tools zur quasi-automatischen Durchsuchung, Sortierung und Aufbereitung von Daten verfügbar. Zum anderen wird der Mangel an qualifizierten und erfahrenen ExpertInnen zur erfolgreichen Verteidigung wichtiger Infrastrukturen den Bedarf nach neuen Machine Learning Technologien ankurbeln, um den Menschen im Kampf gegen Bedrohungen aus dem Cyberspace zu unterstützen.

Menschen können im Fall eines ernsthaften Cyberangriffs zahlreiche aufwändige Verteidigungsschritte nicht in der erforderlichen kurzen Zeit ausführen. Machine Learning ist daher ein wertvolles Werkzeug zur Durchführung von automatisierten Aufgaben wie die Erkennung von Datendiebstahl, die Überprüfung von Zugriffslogs oder Netzwerkverkehr, die Überwachung des Abflusses ungewöhnlicher Mengen sensibler Daten aus dem Netzwerk oder die Verfolgung von Malware-Samples zur Datenexfiltration. Als besonders hilfreich wird sich Machine Learning als Frühwarnmechanismus für Incident Response Teams in 24/7 SOCs (Security Operation Centers) erweisen, indem Gefahren in Echtzeit erkannt werden, noch bevor es zu einem Schaden kommt. Die lernenden Maschinen können frühzeitig einen Überblick über die Situation verschaffen und erlauben es den menschlichen VerteidigungsexpertInnen damit, sich auf die eigentliche Entscheidungsfindung zu konzentrieren.

In gewissem Sinne ist Machine Learning für den Schutz vor Cyberbedrohungen eine spezielle Form der kognitiven Netzwerksicherheit, in der intelligente Systeme eingehende Informationen und Muster analysieren und damit Angriffe bereits im Frühstadium erkennen. IT-SicherheitsexpertInnen können mit diesen technologischen Werkzeugen Angriffe mit Hilfe menschlicher Intelligenz abwehren, gleichzeitig aber auch auf die Unterstützung von Maschinen zurückgreifen, um umfangreiche Datenflüsse zu überwachen und rasch auf Gefahren zu reagieren.

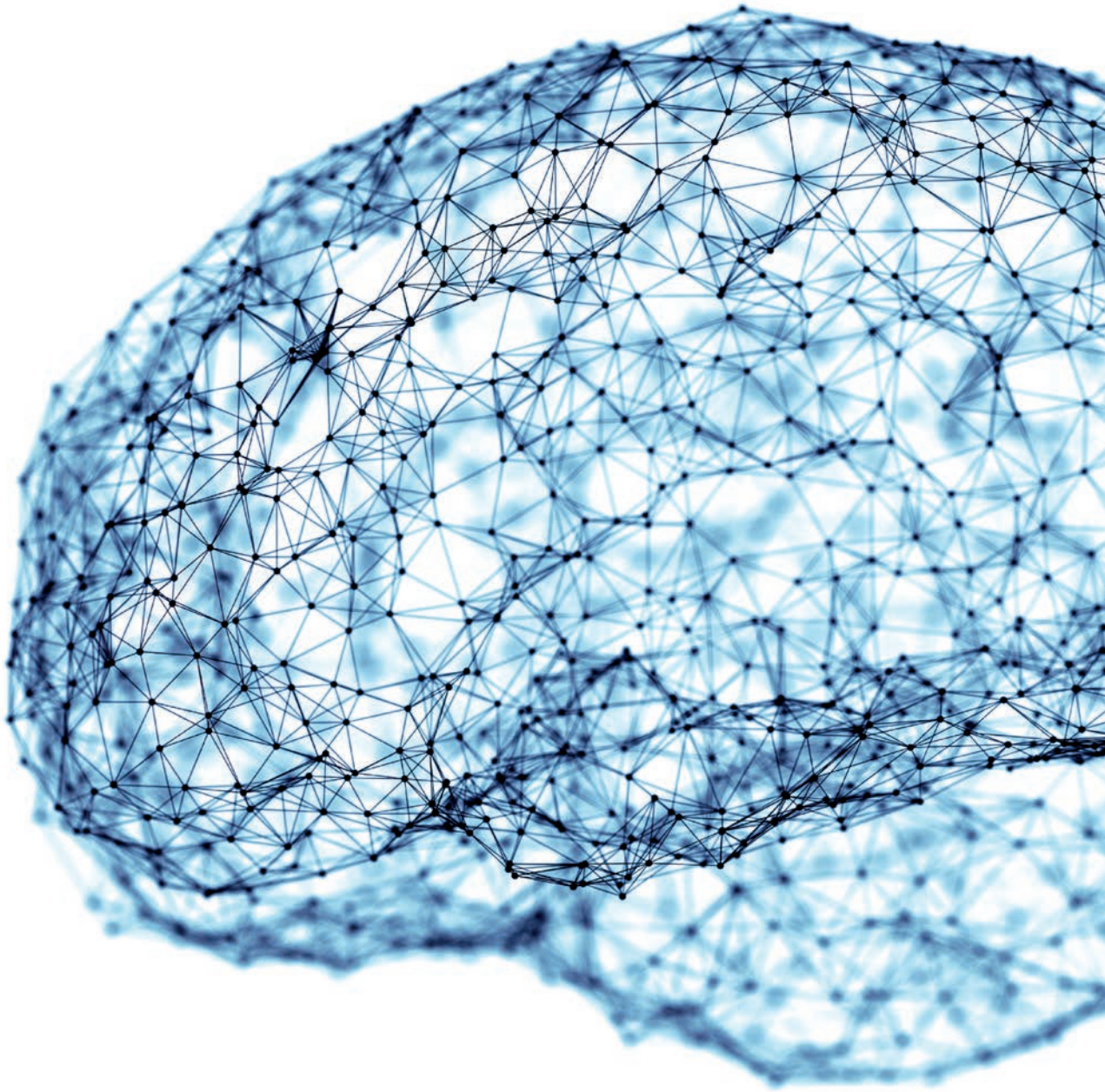
CYBER SECURITY FORSCHUNG AM AIT

Wir am AIT Center for Digital Safety & Security sind uns bewusst, dass angesichts der vielfältigen neuen Cyberbedrohungen eine 100%ige Sicherheit nicht gewährleistet werden kann. Wir können Unternehmen und Verwaltungen jedoch darin unterstützen, die Widerstandsfähigkeit ihrer kritischen Netzwerke und IT-Infrastrukturen zu erhöhen und ihre Assets so gut wie möglich zu schützen.

Unsere Wissenschaftler arbeiten daher an modernsten Machine Learning Technologien und Lösungen für das künftige Cyber Security Ökosystem, um den Bedrohungen entgegenzuwirken, die sich durch neue umfangreiche IKT-Infrastrukturen mit steigender Vernetzung und unklaren Angriffsflächen ergeben. So wurde am AIT mit Automatic Event Correlation for Incident Detection (AECID) eine patentierte Lösung basierend auf Ansätzen aus der Bioinformatik entwickelt, um Systemverhaltensmodelle zu erstellen und relevante Ereignisse und ihre Zusammenhänge besser zu verstehen. Mit unserem selbstlernenden Tool zur adaptiven Verarbeitung von Netzwerk-Logstreams können häufig auftretende Muster in Logfiles und Ereignissen entdeckt, klassifiziert und geclustert und so bekannte „gute" Aktivitäten von unbekannten schädlichen Aktivitäten in betrieblichen IT-Infrastrukturen unterschieden werden.

Die Anwendung versteht Zusammenhänge zwischen Ereignissen über Systeme, Protokolle und Layer unterschiedlicher Abstrahierungsstufen hinweg und verwendet dazu unterschiedliche Mining Instanzen für eine verbesserte Skalierbarkeit. AECID kann auch für Legacysysteme und proprietäre Systeme mit geringer Marktdurchdringung eingesetzt werden. Bereits installierte Sicherheitslösungen müssen nicht ersetzt werden, da AECID parallel dazu läuft und an bestehende SIEM (Security Information and Event Management) Tools angeschlossen werden kann.

AECID ist Teil des AIT-Portfolios für Cyber Security Lösungen, die auf den folgenden Seiten beschrieben werden.



DAS AIT PORTFOLIO INTELLIGENTER CYBER SECURITY LÖSUNGEN

Ein kurzer Überblick über intelligente Sicherheitstechnologien zur Bekämpfung moderner Cyberbedrohungen.

Angesichts ständig komplexerer Cyberbedrohungen werden Cyber Security Unternehmen über kurz oder lang auf selbstlernende Ansätze zurückgreifen müssen, um überleben zu können. ExpertInnen des AIT Center for Digital Safety & Security entwickeln daher in enger Zusammenarbeit mit Organisationen aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung moderne Informations- und Kommunikationstechnologien und -systeme zum Aufbau extrem widerstandsfähiger IKT-Infrastrukturen für die Zukunft. Die Schwerpunkte liegen dabei auf den zentralen Säulen moderner Cyber Security Systeme der nächsten Generation: Risikomanagement, Security by Design und modernste Verschlüsselungstechnologien für virtuelle IoT- und Cloud-Umgebungen, Post-Quanten-computer-Kryptographie, hochzuverlässige sichere Kommunikationstechnologien, Systeme zur Anomalie- und Incidenterkennung mit Hilfe von Machine Learning, Kommunikationstools für den organisationsinternen Informationsaustausch über Cyber-Vorfälle sowie Aktivitäten im Bereich Cyber Range für den Kapazitätsaufbau in relevanten Sektoren wie industrielle Steuerungssysteme (ICS), Fahrzeuge und Industrie 4.0.

Die ExpertInnen des AIT bieten auf dem Gebiet Cyber Security maßgeschneiderte Lösungen, umfassende und langjährige Erfahrung sowie Know-how für national und international geförderte Partnerschaften. Auf der nächsten Seite finden Sie eine Auswahl unserer Forschungs- und Entwicklungsservices.

CYBERSICHERHEIT DURCH MACHINE LEARNING

Die steigende Komplexität unserer IT-Systeme erfordert neue Mechanismen zum Schutz vor ausgeklügelten Cyber-Attacken und zur Erkennung von Anomalien im komplexen Systembetrieb bzw. fehlerhafter Bedienung durch die IT-User selbst. Die ExpertInnen des AIT arbeiten an modernsten Machine Learning Technologien und Lösungen für das künftige Cyber Security Ökosystem, um den Bedrohungen entgegenzuwirken, die sich durch neue umfangreiche IKT-Infrastrukturen mit steigender Vernetzung und unklaren Angriffsoberflächen ergeben.

Im Bereich Blockchain-Technologien arbeiten ExpertInnen an algorithmischen Lösungen, die einen Einblick in Funktionalität und Transaktionsflüsse für die Echtzeitanalyse von virtuellen Währungstransaktionen bieten können. Hauptaugenmerk liegt dabei auf der Erkennung von „Anomalien", also der Identifizierung von Transaktionen und Transaktionsmustern, die von den üblichen Strukturen abweichen. Ziel ist es, die Vorteile moderner Technologien zu nutzen, um potenziellen Missbrauch zu verhindern.

SMART ENCRYPTION FÜR IoT- UND CLOUD-SYSTEME

Große Unternehmen und öffentliche Behörden scheuen oft davor zurück, ihre sensiblen Daten außenstehenden Stellen zur Speicherung und Verarbeitung zu überlassen. Die ExpertInnen des AIT arbeiten an Konzepten der agilen Verschlüsselung, um einen besseren Datenschutz in der Cloud zu gewährleisten. Sie entwickeln sichere Cloud-Services zur Unterstützung der gemeinsamen Arbeit an verschlüsselten Daten, d.h. selektive fein granulierte Zugriffskontrolle und integrierte Resilienz. Darüber hinaus entwickeln sie Technologien zur Verbesserung des Datenschutzes für den Aufbau von zuverlässigen Identitätsmanagementsystemen und datenschutzfreundlichen intelligenten Anwendungen für Cloud Computing und das Internet of Things (IoT).

SECURITY BY DESIGN FÜR KRITISCHE INFRASTRUKTUREN

Die mit der Einführung von Smart-Grid-Technologien einhergehende Vernetzung von bisher isolierten Komponenten bringt zwei wesentliche Herausforderungen mit sich: zum einen muss die Interoperabilität von Komponenten verschiedener Systemebenen und/oder Hersteller gewährleistet sein, zum anderen muss das Smart Grid eine hohe Resilienz gegen Cyber-Angriffe aufweisen. Im Rahmen der österreichischen Initiative zur Definition einer Referenzarchitektur für sichere Smart Grids in Österreich (RASSA) entwickelten AIT ExpertInnen gemeinsam mit relevanten Stakeholdern wie z.B. Netzbetreibern, Herstellern, Energieversorgern, Regulatoren und öffentlichen Bedarfsträgern Methoden und Tools zur Modellierung einer Referenzarchitektur für zukünftige sichere Smart Grid Lösungen.

AIT KAPAZITÄTSAUFBAU UND TECHNOLOGIE-VALIDIERUNG

Sicherheit ist nicht nur eine Frage der Technologie – sie umfasst darüber hinaus auch Prozesse, Bedienbarkeit, operative Fähigkeiten und ein Verständnis der Systemkomplexität. Zum Zweck des Wissenstransfers hat das AIT in Kooperation mit der Internationalen Atomenergiebehörde (IAEA) ein "Cyber Range" Trainingszentrum aufgebaut, in dem Stakeholder aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung ausgebildet und auf einen gemeinsamen Wissensstand gebracht werden. Eine Cyber Range ist eine virtuelle Umgebung für die flexible Simulation großer, komplexer Netzwerke mit verschiedenen Systemkomponenten, Netzen und Nutzern. Sie bietet eine sichere und realistische Umgebung zur Erprobung, Untersuchung und Analyse von Vorfällen in unterschiedlichen skalierbaren Szenarien, ohne auf tatsächliche Produktionssysteme zurückgreifen zu müssen. Mit ihrer flexiblen Architektur kann eine Cyber Range für unterschiedliche Anwendungen eingesetzt werden, so etwa für Ausbildung, Evaluierung von Incident Response Prozessen und Softwaretests. Dadurch können Forscher und Stakeholder aus Wirtschaft und öffentlicher Verwaltung zusammen in einem realitätsnahen Umfeld Methoden, Technologien und Prozesse für einen wirksamen Schutz vor Cyberattacken entwickeln, implementieren und validieren.

INTERNATIONALE SCHUTZMECHANISMEN AUF UNTERNEHMENSEBENE

Cyberattacken, ob mit kriminellen, geheimdienstlichen, terroristischen oder sogar kriegerischen Absichten, werden immer professioneller und ausgeklügelter geführt. Eine hohe Widerstandsfähigkeit gegen Bedrohungen dieser Art ist mittlerweile ein zentraler Erfolgsfaktor für moderne Unternehmen.

INTERNATIONALE CYBER SECURITY INITIATIVEN

Auf EU und nationaler Ebene wurden verschiedene Maßnahmen ergriffen, um ein europäisches System zum Schutz vor Cyberangriffen zu etablieren. Die EU hat eine Cybersicherheitsstrategie[3] sowie Empfehlungen[4] zur Prävention und Reaktion im Falle von Störungen und Angriffen auf kritische Infrastrukturen in Europa definiert. Um die Widerstandsfähigkeit unserer digital gesteuerten Infrastrukturen zu erhöhen, diskutieren Unternehmen und Organisationen unter anderem spezielle Strukturen für ein Cyber Security Management auf staatlicher Ebene, ein Mindestsicherheitsniveau auf Unternehmensebene sowie eine Meldepflicht für ernsthafte Cybervorfälle. Außerdem trat im August 2016 die NIS-Richtlinie[5] der EU zur Umsetzung nationaler Cybersicherheitsgesetze in Kraft.

In Österreich wird 2018 ein vom Bundeskanzleramt (BKA), dem Innenministerium (BMI) und dem Ministerium für Verteidigung und Sport (BMLVS) ausgearbeitetes Gesetz in Kraft treten[6]. Ebenfalls im nächsten Jahr, am 25. Mai 2018, wird ein europaweites EU-Datenschutzrecht in Kraft treten. Unternehmen müssen dann verpflichtend nachweisen, dass ein ausreichender Schutz persönlicher Daten gewährleistet ist. Die Schutzmaßnahmen umfassen Risikoanalysen ebenso wie die Einführung von Cybersicherheitssystemen.

SCHUTZMASSNAHMEN DER INDUSTRIE

Zur Adressierung dieser umfassenden Sicherheitsaspekte sind fünf zentrale Punkte für die Industrie wesentlich:

- Schaffung eines tiefgreifenden Verständnisses von Digitalisierungstechnologien und zentralen Sicherheitsaspekten
- Neudefinition der Prioritäten: für die gesamtheitliche Systemsicht sind neue Fähigkeiten und neue Prozesse erforderlich
- Aufbau einer zeitgemäßen Risikomanagementstrategie zur effizienten und gezielten Umsetzung geeigneter Schutzmaßnahmen
- Eingebaute Sicherheit und Datenschutz durch frühzeitige Einbindung von Sicherheitskonzepten in Systemlösungen
- Koordinierter Einsatz neuester Angriffserkennungssysteme und Verteidigungstools zum Schutz vor Internetbedrohungen sowie eine gemeinsame Verteidigungsstrategie

[3] http://www.consilium.europa.eu/de/policies/cyber-security/
[4] http://www.spiegel.de/netzwelt/netzpolitik/cyber-gesetz-eu-kommission-einigt-sich-auf-nis-richtlinie-a-1066642.html
[5] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[6] http://www.bmi.gv.at/cms/cs03documentsbmi/1326.pdf

EIN STATE-OF-THE-ART SCHUTZSCHILD

GRUNDLEGENDE ASPEKTE EINER SICHERHEITS-INFRASTRUKTUR FÜR MODERNE UNTERNEHMEN

Beim Aufbau und Betrieb einer modernen unternehmensweiten Sicherheitsinfrastruktur müssen folgende Sicherheitskategorien und –aspekte berücksichtigt werden.

CYBER SECURITY TEAM

Ein Unternehmen benötigt zuallererst ein eigenes Team, das sich tagtäglich ausschließlich mit Sicherheitsaspekten befasst. Dieses Team hat die Aufgabe, das Netzwerk zu organisieren, die Netzwerkeinheiten zu betreiben und sämtliche Elemente des Netzwerks (Firewalls, etc.) an die jeweiligen Arbeitsabläufe und –routinen anzupassen. Nicht zuletzt ist das Team aber auch dafür verantwortlich, abnormales Verhalten im Netzwerk zu analysieren, Log-Dateien von Firewalls und Servern zu interpretieren und erkannte Angriffe abzuwehren.

RISIKOMANAGEMENT

Kritische Infrastrukturen werden immer abhängiger von Informations- und Kommunikationstechnologien. Damit steigt auch die Bedrohung durch Cybersicherheitsrisiken in allen Wirtschaftszweigen, vor allem in den Bereichen Energie, Fahrzeug, Gesundheit und Produktion. Die Infrastrukturbetreiber müssen sich kritische Fragen stellen, z.B.:

- Was passiert, wenn Daten gestohlen oder unerlaubt weitergegeben werden? Was passiert, wenn das System ausfällt, außer Kontrolle gerät oder geändert wird?
- Wie kann ich Fehlverhalten erkennen? Oder Modifikationen? Oder Löschungen?
- Wie erlange ich die Kontrolle über ein System zurück, das sich in einem unkontrollierbaren Zustand befindet?

Als Antwort darauf bietet das AIT Technologien und Tools zur Stärkung der Widerstandsfähigkeit kritischer Infrastrukturen (z.B. Smart Grids) gegen Cyberangriffe. Das Portfolio umfasst spezielle Risikomanagement-Ansätze für Versorgungsunternehmen, Prozesse und Richtlinien für Sicherheitsmaßnahmen in Infrastrukturen sowie Lösungen für Security Assessments und Systemüberwachung.

SECURITY BY DESIGN

Bei der Entwicklung von modernen IKT-Systemen müssen Sicherheitsmaßnahmen von Anfang an integriert werden. Neue Methoden und Tools für eine sichere und effiziente Systementwicklung und -implementierung sind daher gefragt. Die entwickelten Methoden nutzen vorhandene Technologien wie Kryptographie und Federated Identity Management sowie innovative Ansätze wie modellbasierte Sicherheitskonzepte, um Vertraulichkeit, Integrität und Verfügbarkeit in großen verteilten Systemen sicherzustellen. Ein System ist nur so sicher wie sein schwächstes Glied. Aus diesem Grund muss die Integration von Sicherheitsmaßnahmen in den verschiedenen Phasen der Systementwicklung einfach und effizient möglich sein, um breite Anwendung zu finden. AIT entwickelt dafür „Security by Design"-Architekturen und unterstützende Tools für eine sichere Softwareentwicklung, vom Design über die Implementierung bis hin zur Validierung.

KRYPTOGRAPHIE

Internetbanking, sichere Bezahlsysteme, digitale Unterschriften - ohne den Einsatz moderner Kryptographie sind all diese Errungenschaften undenkbar. Für das Design von sicheren und intelligenten Kommunikationssystemen der nächsten Generation ergeben sich daraus viele neue Herausforderungen, die vor allem auch neue Ansätze in der Kryptographie erfordern. Deshalb wird am AIT an neuen kryptographischen Verfahren geforscht, um IKT-Systeme in Zukunft sicherer zu machen. Die entwickelten Methoden, Konzepte und Prototypen sollen die Daten und die Privatsphäre der Benutzer bei der Interaktion mit IKT im Kontext von Cloud Computing und dem Internet of Things (IoT) besser schützen.

CLOUD SECURITY

Cloud Computing ist einer der wichtigsten IT-Trends der letzten Jahre. Aus diesem Grund investieren bedeutende Firmen massiv in Cloud Infrastrukturen. Cloud Computing betrifft viele Aspekte aktueller IT-Unternehmensinfrastrukturen (z.B. Sicherheitsmanagement in Organisationen, Facility Management, rechtliche Rahmenbedingungen), führt aber auch zu wachsenden Bedenken in Bezug auf Sicherheit, Zuverlässigkeit und Informationssicherheit. Am AIT werden daher modernste Konzepte, Methoden und Technologien für die Realisierung geschützter, zuverlässiger und hochsicherer Cloud Computing Umgebungen für kritische IT-Infrastrukturen entwickelt.

SAFETY & SECURITY CO-DESIGN

Vernetzte eingebettete Systeme, die in die physische Umgebung integriert sind, werden als Cyber-Physical Systems (CPS) bezeichnet. Diese Systeme sind die treibende Kraft hinter einer Vielzahl von technologischen Innovationen zur verbesserten Effizienz, Funktionalität und Zuverlässigkeit von Produkten, Services und Infrastrukturen. Unsere Gesellschaft wird immer abhängiger von diesen "intelligenten" Systemen, die in smarten Haushaltsgeräten ebenso zum Einsatz kommen wie in Industriesteuerungen, Smart Cities und intelligenten Transportsystemen.

Aufgrund des Umfangs, der Komplexität und Vernetzung dieser Systeme stellt es eine große Herausforderung dar, ihre Sicherheit und Widerstandsfähigkeit zu gewährleisten. Fehler und Störungen sowie bösartige Angriffe können ein System zum Erliegen bringen und verheerende Konsequenzen in der physischen Welt nach sich ziehen, die sämtliche Vorteile der Technologie zunichtemachen. Da Systemfeatures immer stärker von Rechnern, Netzwerken und Informationsverarbeitung abhängig sind, sind Ausfallsicherheit (Safety) und Datensicherheit (Security) in CPS sehr eng miteinander gekoppelt. Ausfallsicherheit kann ohne Datensicherheit nicht garantiert werden.

Ein integrierter Prozess für Cyber Security und Safety erlaubt Zugriff auf ein gemeinsames Ressourcenset und benötigt daher weniger zusätzliche Ressourcen. AIT beteiligt sich aktiv an Standardisierungsaktivitäten, um Safety & Security Co-Design und gemeinsame Ansätze zu fördern.

CHECKLISTE FÜR CYBERSICHERHEIT

Die wichtigsten Maßnahmen für Organisationen lassen sich in drei Kategorien unterteilen: Netzwerk, Daten und Menschen. Mit der folgenden Checkliste können Sie den aktuellen Stand der Cybersicherheit Ihrer Infrastruktur bestimmen.

NETZWERKMANAGEMENT

1. Netzwerkabschnitte gemäß Sicherheitsplan
Kritische Bereiche sollten (auch physisch) vom normalen Netzwerk getrennt werden. Lassen Sie nur einige wenige Verbindungspunkte zu. Vermeiden Sie unbelegte Zugangspunkte, an denen ein Computer angeschlossen werden könnte.

2. Effektives Domain-Management
Wenn Nutzer keinen Zugang zu einem bestimmten Netzwerk oder Computer benötigen, sollten Sie ihnen diesen auch nicht gewähren. Nicht alle Arbeitsplatzrechner müssen mit anderen Rechnern verbunden sein. Wenn Nutzer nur fallweise Zugang zu einem bestimmten Netzwerk benötigen (z.B. für die Wartung), sollten sie andere Accounts benützen.

3. Zugriffssteuerung nach dem Least-Privilege Prinzip
Zugriffsrechte sollten nur mit Zustimmung des Dateneigentümers gewährt und alle Berechtigungen regelmäßig überprüft werden. Vermeiden Sie die Möglichkeit, Zugriffsrechte für alle User zu vergeben, vor allem in Cloud-Umgebungen.

4. Rollenbasierte Zugriffskontrolle (RBAC)
RBAC (role-based access control) ermöglicht eine Zugriffskontrolle nach dem Least-Privilege Prinzip basierend auf erlaubten Handlungen und Benutzerrollen. In RBAC-Systemen werden Zugriffsrechte an rollenbasierte Gruppen und nicht an User Accounts oder Abteilungsgruppen vergeben.

DATENMANAGEMENT

1. Verhinderung von Datenlecks
Wirksame Monitoringsysteme können den unerlaubten Zugriff oder Transfer von Daten verhindern. Sie müssen so konfiguriert werden, dass sie unerlaubten Datenzugriff erkennen, ohne jedoch zu viele falsche Treffer zu generieren. Noch wichtiger ist, dass jemand die Systeme überwacht und auf die von ihnen gelieferten Informationen reagiert.

2. Verschlüsselung
Verschlüsseln Sie sensible Daten sowohl bei der Übertragung als auch bei der Speicherung (auch auf Speichermedien wie tragbaren Festplatten und USB-Sticks).

3. Sicherheitsmaßnahmen von Anfang an integrieren
Unzureichende Standardsicherheitseinstellungen und falsche Konfigurationen sind der Grund für viele Sicherheitsvorfälle. Es muss daher sichergestellt werden, dass alle Computer nach dem neuesten Stand der Technik konfiguriert sind.

MENSCHEN

1. Grundlegende Hintergrundprüfungen
Viele interne Angriffe gehen auf das Konto von Wiederholungstätern. Organisationen sollten ihre Angestellten Hintergrundüberprüfungen unterziehen und bei entsprechender Verdachtslage Informationen bei früheren Arbeitgebern einholen.

2. Benutzungsrichtlinien
Die Erstellung einer Benutzungsrichtlinie ist eine hilfreiche Maßnahme, um das von den Arbeitnehmern erwartete Verhalten festzulegen. Die Arbeitnehmer sollten eine Vereinbarung unterzeichnen, in der festgehalten wird, dass unerlaubter Datenzugriff ein schwerwiegendes Vergehen darstellt. Es sollte über die Wahl von sicheren Passwörtern, physische Schutzmaßnahmen und Gefahren durch externe Festplatten aufgeklärt werden.

3. HR: ganzheitliche Beendigungsverfahren
Jedes Unternehmen sollte über standardisierte Verfahren zur Beendigung von Arbeitsverhältnissen verfügen. Dazu zählen die sofortige Sperrung der Zugangsrechte zu Gebäuden und Zugriffsrechte auf digitale Netzwerke.

4. Rollen-/Funktionsbasierte Zugriffsrechte
Ändert ein Arbeitnehmer seine Rolle innerhalb der Organisation, sollte das Unternehmen die Zugriffsrechte formell neu überprüfen, um sicherzustellen, dass diese Berechtigungen nicht einfach akkumulieren. Passwörter, die dem Arbeitnehmer in seiner früheren Rolle oder Funktion bekannt waren, sollten geändert werden. Vergeben Sie nur individuelle Passwörter.

5. Supply Chain & Vereinbarungen mit Dritten
Eine nicht unerhebliche Anzahl von Datenschutzverletzungen geht auf das Konto von vertrauenswürdigen Dritten. Diese sollten daher Benutzungsrichtlinien unterschreiben und nur Programme benützen, die den üblichen Sicherheitskriterien (Firewalls, Virenschutz, etc.) entsprechen.

6. Trennung von Rolle und Funktion
Verhindern Sie mit entsprechenden Richtlinien, dass ein einziger Arbeitnehmer seine Befugnisse missbrauchen kann, um dem Unternehmen beträchtlichen Schaden zuzufügen. So sollten etwa Accounts mit hoher Berechtigungsstufe vom normalen Account des Nutzers getrennt werden. Das heißt: unterschiedliche Accounts für unterschiedliche Aufgaben.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Markus Kommenda
Business Development
Center for Digital Safety & Security
Phone +43 50550 4180
Donau-City-Straße 1, 1220 Wien, Austria
markus.kommenda@ait.ac.at
www.ait.ac.at

Produktionsmanagement: Michael Mürling; Bilder: iStock.com, AIT