IT Security

Knowhow für das Unternehmensmanagement

IT-SICHERHEIT 2025:

Das erwarten Experten für die Zukunft

INNOVATION & SECURITY IM „FLIEGENDEN RECHENZENTRUM“

Dr. Roland Schütz CIO, Lufthansa Group Airlines im Interview

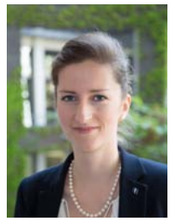
Strategien – Technologien – Organisation & Compliance

Mensch versus Maschine: Wie selbstlernende Systeme Cyberangriffe erkennen

AUSGABE 1

powered by RADAR SERVICES

Was erwartet uns in der Zukunft?



Liebe Leserinnen und Leser,

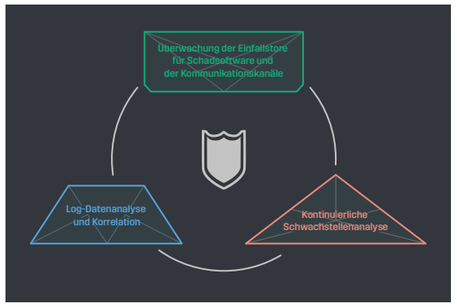
was erwartet uns in der Zukunft? Das ist eine besonders interessante Frage, wenn es um langfristige Investitionsentscheidungen und strategische technologische Kooperationen geht. Und genau darum geht es in der IT-Sicherheit. Die zunehmende Komplexität und Dynamik technologischer, aber auch wirtschaftlicher und gesellschaftlicher Systeme, die steigenden Performanceerwartungen genauso wie ein anhaltender Kostendruck tragen zu einem starken Interesse an – möglichst verlässlichen – Aussagen über die Zukunft bei.

Nun ist das Vorhersagen von zukünftigen Ereignissen meist ein eher schwieriges Unterfangen. Am besten fragt man aber die, die Zukunft mitgestalten: Die Expertinnen und Experten ihrer Branche. Einen Auszug aus deren Antworten, die sie uns in der aktuellen Studie zum Thema gegeben haben, präsentieren wir Ihnen in dieser Ausgabe. Ausführlich zu Wort kommt Dr. Roland Schütz, CIO der Lufthansa Group Airlines und gibt einen Einblick in die „fliegenden Rechenzentren“ von heute und morgen. Im Fokus der Ausgabe ist auch das zentrale Forschungsthema in unserer Branche: selbstlernende Systeme zur IT-Risikoerkennung.

In „IT Security – Knowhow für das Unternehmensmanagement“ werden die Themen rund um die IT-Sicherheit so aufbereitet, dass sie nicht nur Fachleute verstehen. Unser Anspruch ist es, die Themen auch für Leserinnen und Leser aus anderen Branchen interessant und verständlich zu gestalten.

In diesem Sinne wünsche ich Ihnen eine spannende Lektüre.

Ihre Isabell Claus, Herausgeberin



Organisierte Cyberkriminalität:
Die 3 „Must-haves“ für die zeitnahe Erkennung von gezielten Cyberangriffen **S. 22**

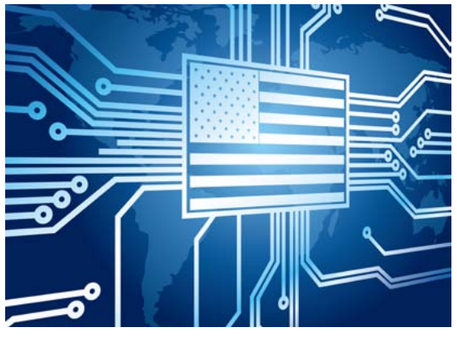
2025: Innovation steht und fällt mit dem Fortschritt der IT-Sicherheit **S. 6**

Innovation & Security im „fliegenden Rechenzentrum“ – Interview mit Dr. Roland Schütz, CIO, Lufthansa Group Airlines **S. 12**

Cyberattacken und IT-Sicherheitsmanagement in 2025 **S. 18**

Mensch versus Maschine: Wie selbstlernende Systeme Cyberangriffe erkennen **S. 24**

Sicher wie Fort Knox? Warum selbst fortschrittlichste Institutionen anfällig für Cyberangriffe sind **S. 26**



Datenübertragung in die USA: IT-Sicherheit darf sich auch im Cloud-Zeitalter nicht in Luft auflösen **S. 30**

INHALT

2025

Innovation steht und fällt mit dem Fortschritt der IT-Sicherheit

iStock.com/a+ ct·st

Die fortschreitende Digitalisierung verändert das Leben und die Wirtschaft bis 2025 nachhaltig. Die Grundlagen dafür sind schon geschaffen, die Visionen umrissen. Die neuen Möglichkeiten, die Informations- und Kommunikationstechnologien eröffnen, haben längst einen entscheidenden Einfluss auf uns, die Erforschung der Welt und die Nutzung der Ressourcen genommen. Und es geht weiter. Die Abhängigkeit von der Technologie wächst.

Mit sich bringt das die Frage des Vertrauens in diese Technologie. Bleiben vertrauliche Informationen vertraulich? Funktionieren IT-Systeme immer so wie sie sollen? Können unautorisierte Personen unbemerkt die Kontrolle über Rechner übernehmen, Daten entwenden oder Schaden anrichten?

Ein Blick in die Zukunft verschiedener Gesellschafts- und Wirtschaftsbereiche zeigt die großartigen Entwicklungen aber auch Herausforderungen, die die allumfassende Digitalisierung mit sich bringt. Und: Die einhergehende Bedeutung von IT-Sicherheit, die heutiges und zukünftiges Vertrauen in und damit die Akzeptanz von Technologie erst ermöglicht.

Mehr Menschen, mehr digitale Erreichbarkeit

Die UNO rechnet mit einer Weltbevölkerung von 8 Milliarden Menschen in 2025. Das ist knapp eine Milliarde Menschen mehr als heute. Das schnelle Bevölkerungswachstum in China, Indien und Afrika

2016

Das „Freedom 251“, mit 4 USD das billigste Handy der Welt, kommt in Indien auf den Markt, Nachfrage in den ersten Tagen: 70 Millionen Stück

(Quelle: Ringing Bells)

bedeutet hohes Wirtschaftswachstum. Einerseits wird die gesellschaftliche Mittelschicht stark zunehmen und die Nachfrage, zum Beispiel nach Technologie, damit steigen. Andererseits arbeiten Unternehmen wie Google daran, Zugang zu Informations- und Kommunikationstechnologie allen Menschen weltweit zu ermöglichen.

2020

Datenexplosion: Das Volumen der generierten digitalen Datenmenge weltweit wächst von derzeit jährlich 8.500 auf 40.000 Exabyte

(Quelle: Statista)

Das Internet of Things verbindet alles um uns herum

Physische Objekte sind mit dem Internet verbunden und ermöglichen durch integrierte Sensoren, Chips und Software eine Fernüberwachung ihrer Leistung und ihres Umfeldes. Sie schaffen eine neue Realität: Innovationen im Gesundheitsbereich unterstützen Früherkennung, Diagnosen und Behandlungen. Das Auto wird (noch) intelligenter: „Schwarmintelligenz“

2020

Mehr als die Hälfte aller großen Geschäftsprozesse werden mit dem Internet der Dinge vernetzt sein

(Quelle: Gartner)

vermeidet Unfälle, spart Zeit, Geld und Energie und schon bald realisiert sich die Vision vom selbstfahrenden Auto in Massenproduktion. Im „Haus von morgen“ werden Heizung und Klimatisierung kontinuierlich überwacht, Kühlschränke denken fürs Einkaufen mit und alle Geräte werden vom Smart Phone (fern-) gesteuert.

Industrie 4.0 revolutioniert Produktion und Logistik
Die vierte industrielle Revolution ist in vollem Gang. „Smart Objects“ kommunizieren miteinander und ermöglichen die Selbststeuerung von Fertigungsanlagen oder ein echtzeitnahes Supply Chain Management. Daneben wird auch die Logistik wesentlich weiterentwickelt: Antizipatorische Lieferungen werden Realität und Distributed Order Management versetzt Anbieter in die Lage, jede Bestellung von jedem ihrer Standorte zu bedienen – basierend auf den Überlegungen zu Kundennutzen und Profitabilität.

2020

In Deutschland wird ein Anstieg des Digitalisierungsgrades bei Produktionsprozessen von heute 33% auf 82% erwartet

(Quelle: PWC)

Disruptive Innovationen in der Finanzindustrie
Bitcoins haben eine Revolution des Zahlungsverkehrs eingeleitet. Zentralbanken, Großbanken und die Forschung erkennen das Potential. Sie arbeiten daran, auf der Basis der Blockchain, die hinter Bitcoin steht, eine weiterentwickelte, universell einsetzbare Währung zu gestalten.

Während sich mit Blockchains derzeit hauptsächlich Spezialisten auseinandersetzen, werden Kunden von Finanzdienstleistern im Allgemeinen immer technologie-affiner und nutzen mehr und mehr onlinebasierte Dienstleistungsplattformen. Daten und das daraus generierte Wissen über Kunden, ihre Wünsche und Bedürfnisse sind für eine umfassende, langfristige und individuelle Betreuung zentral.

Die Macht dieser Daten und ihre Anwendung wird auch durch den Vormarsch von FinTechs ersichtlich. Die rasant wachsenden Start-Ups stellen Technologie in den Mittelpunkt und erbringen Finanzdienstleistungen damit wesentlich schneller und preiswerter. Andererseits drängen Nicht-Finanzinstitute wie Facebook, Amazon und Google mit ihrem umfangreichen Wissen über ihre Klientel traditionelle Banken zur Neudefinition.

Energieversorgung neu gedacht und smart gemacht
Die Energielandschaft der Zukunft besteht aus erneuerbaren Energien, einer dezentralen Energiegewinnung und Smart Grids, den intelligenten Stromnetzen. Datensammlung und –austausch sind die Basis für ihr Funktionieren und die Grundlage für nachhaltige Geschäftsmodelle von Energieunternehmen. Unterstützt durch digitale Plattformen werden Endverbraucher in der Lage sein, ihre Stromversorgung gezielt zu beziehen. Und: Stromnetze werden sich selbst verwalten

2025

Technologie ersetzt 30% der derzeitigen Arbeitsplätze in US-Banken

(Quelle: Citigroup)

2025

Fast die Hälfte der in Deutschland benötigten Elektrizität basiert auf erneuerbaren Energien, die „smart“ gemanagt werden.

(Quelle: Deutsches BMWI)

und konfigurieren, auf Spannungsänderungen durch Selbsteinstellung eingehen und Störungen durch Selbstoptimierung abmildern können.

Die dunkle Seite der Digitalisierung

Die Digitalisierung macht Maschinen, Komponenten und Technologien besser in Prozesse integrier- und steuerbar und lässt die intelligente Vernetzung und Technisierung in alle Lebensbereiche einziehen. Einher geht eine Datenexplosion.

Doch wie geht es den Menschen damit? Wo Licht ist, ist auch Schatten. Und so können die revolutionäre Technologie, die Vernetzung und die Zetabytes an Daten nicht nur für Fortschritt eingesetzt werden. Sie machen Menschen, Wirtschaftssysteme und Unternehmen auch angreifbar.

So bleibt bei aller Veränderung eines bestehen: Ein dauerndes Wettrennen zwischen Cyberangreifern und IT-Sicherheitsbereichen von Unternehmen und Organisationen. Angriffe entwickeln sich dabei in zwei Richtungen: komplexe, gezielte Cyberattacken mit wachsendem Schadenspotential für attackierte Unternehmen, Wirtschaft, Gesellschaft oder Staat und automatisierte Massenangriffe. Für beides müssen Unternehmen gewappnet sein. Auf dem Spiel steht nichts Geringeres als ihr guter Ruf und im schlimmsten Fall ihre Existenz. Im Fokus bleibt die Finanzbranche mit all ihren digitalen Entwicklungen, gleich gefolgt von der Industrie mit ihren stark vernetzten Produkten und Prozessen.

IT-Sicherheit in 2025
5 Zukunftsthesen

1. UNTERNEHMEN ÜBERNEHMEN EINE ALLUMFASSENDE VERANTWORTUNG FÜR DIE IT-SICHERHEIT

IT-Sicherheit ist und wird für ein großes Kraftwerk genauso wichtig wie für einen wenige Millimeter kleinen, digitalisierten Herzschrittmacher. Der Unterschied zu heute liegt aber in der Verantwortlichkeit, für die IT-Sicherheit zu sorgen: Der Kraftwerksbetreiber wird auch weiterhin die Verantwortung für seine Anlage tragen. Der Herzpatient hingegen muss auf den Hersteller seines Schrittmachers vertrauen. In der stark vernetzten Welt spielen also Unternehmen – Hersteller oder Betreiber – die zentrale Rolle für IT-Sicherheit. Verbraucher haben auf IT-Sicherheit nahezu keinen Einfluss mehr. Der Einsatz einer Anti Virus-Software auf einem Privat-PC vermag heute noch ein Sicherheitsgefühl erzeugen, in 2025 geht von diesem PC wahrscheinlich die kleinste Gefahr aus. Stattdessen wird der Anspruch an Hersteller bestehen, die Sicherheit bereits im Entwicklungsprozess zu bedenken, in die Technologie oder das Produkt von vornherein zu integrieren und laufend auch den neuesten Gefahren und bekannt werdenden Schwachstellen anzupassen.

2. IT-SICHERHEIT BERUHT AUF EINEM FRÜHWARNSYSTEM MIT GANZHEITLICHEM ANSATZ UND HOHEM AUTOMATISIERUNGSGRAD

Datenschutz wird zum größten Anspruch von Staaten an ihre Unternehmen und gleichzeitig zu deren herausforderndster Aufgabe. Denn vertrauliche Daten werden immer interessanter und Angreifer gibt es auf allen Ebenen, nicht zuletzt gehen Gefahren von Staaten selbst aus. Der Drang, Wirtschaftszweige im eigenen Land zu stärken, führt zu digitaler Spionage und Diebstahl von Intellectual Property. IT-Frühwarnsysteme mit ganzheitlichem Ansatz zur weitgehend automatisierten Erkennung und Verhinderung von Abflüssen sensibler Daten bilden die vielversprechendste Lösung. Basierend auf ihrem Wissen über ein aktuelles Gesamtlagebild zu im Umlauf befindlicher Schadsoftware und kriminellen Gruppen werden sie bereits daraus resultierende Bedrohungen erwarten und die richtigen Prozesse einleiten. Möglich wird das bis zu einem gewissen Grad durch selbstlernende Systeme (Machine Learning). Experten-Knowhow wird dennoch nicht vollständig ersetzt werden können.

3. IT-SICHERHEIT BLEIBT SPEZIALISTENTUM, DER „WAR FOR TALENTS“ BLEIBT INTENSIV

Die Arten von Angriffen und verwendeten Technologien ändern sich laufend, die Komplexität steigt. Die Erkennung von und Reaktion auf Gefahren müssen dem

angepasst sein. IT-Sicherheitsexperten stehen also unter ständigem Druck, sich weiterzubilden, neueste Erkenntnisse aus der Branche und branchenübergreifend zu studieren, mit neuen Technologien zu experimentieren und sich immer tiefer in Teilgebieten der IT-Sicherheit zu spezialisieren. Die Beschäftigung dieser Experten wird für Unternehmen, für die IT-Sicherheit nicht das Kerngeschäft ist, kostenintensiv und zunehmend unwirtschaftlicher. Gleichzeitig wird es für die Experten interessanter, ihre Fähigkeiten für mehrere Unternehmen einzusetzen und so ständig neue Praxisfälle zu bearbeiten. Managed Security Operations Centers, also externe IT-Sicherheitsdienstleister, ziehen die Nachwuchstalente an.

4. TRANSPARENZ SPIELT DIE ZENTRALE ROLLE IM IT-SICHERHEITSMANAGEMENT

Die global verteilte Unternehmens-IT muss rund um die Uhr verlässlich zur Verfügung stehen. Informationen werden 24 Stunden verarbeitet, Prozesse greifen über Kontinente hinweg ineinander. Stehen IT-Services still, stehen ganze Geschäftsprozesse still. Transparenz im IT-Sicherheitsmanagement spielt zur Vermeidung dieses Szenarios und – falls notwendig auch zu seiner Behebung – die zentrale Rolle. Sie schützt vor langen Ausfällen und ermöglicht schnelles Handeln im Notfall. Mit Hilfe neuer Protokolle und Technologien gibt sie den Sicherheitsverantwortlichen einerseits und dem Management andererseits einen zentral abrufbaren, tagesaktuellen Überblick über die IT-Sicherheit des Gesamtunternehmens, also inklusive allen Geschäftsbereichen, den IoT-Technologien, der IT-Infrastruktur und allen Netzen.

5. INVESTITIONEN IN IT-SICHERHEIT WERDEN HÖHER SEIN ALS HEUTE, ABER SIE WERDEN ERFOLGSBASIEREND STEUERBAR

Mehr Transparenz führt nicht nur zu mehr Klarheit über den Einfluss von IT-Sicherheit auf Geschäftsprozesse. Vielmehr rechtfertigen die genauen Informationen über vermiedene Ausfälle, Schäden oder Verluste die getätigten Investitionen in die IT-Sicherheit. Der heute oft schwer ersichtliche Nutzenbezug der aufgewendeten Ressourcen wird erkennbar. Damit werden Kennzahlen, Gesamtrisikowerte und Trendanalysen in Balanced Score Cards und Management Cockpits integriert und erfolgsbasierend steuerbar.

Fazit

Innovation basierend auf Digitalisierung macht die Welt von morgen schneller, besser und effizienter. Doch dabei rückt IT-Sicherheit in den Fokus. Es ist ihr Fortschritt, der den Erfolg von Innovation langfristig erst möglich macht. Denn Innovation bedeutet, dass sich Neues auch am Markt durchsetzen muss. Und das passiert nur, wenn Menschen sich beim Einsatz des Neuen sicher fühlen, ihm vertrauen.

Wie groß der Fortschritt der IT-Sicherheit bis 2025 tatsächlich sein wird, hängt ganz zentral davon ab, wie gut sich Unternehmen schon heute auf die Zukunft vorbereiten.

Fotograf: Oliver Rösler für Lufthansa Deutschland

Herr Dr. Schütz, welche Rolle spielt IT heute in der Luftfahrt?

Bei den IT-Landschaften von Fluglinien, Flugsicherung und Flughäfen handelt es sich heute um komplexe Zahnradsysteme, die perfekt ineinandergreifen müssen. Die weltweite Vernetzung und Integration von Systemen ist in unserer Branche unerlässlich. Systemausfälle oder streckenweise Störungen im Luftverkehr verursachen Flugverschiebungen und -ausfälle, die mit immensen Kosten verbunden sind. Die hohe Verfügbarkeit unserer Leistungen – rund um die Uhr, 365 Tage im Jahr – ist daher eine Grundvoraussetzung.

Die meisten Berührungspunkte mit unseren Passagieren werden durch die IT bestimmt, egal ob Check-in, Entertainment an Bord, die Überprüfung des Gepäckstatus, das Abrufen zusätzlicher Reiseinformationen oder die Navigation an Großflughäfen. Vollautomatische Check-in-Prozesse mit Gepäckautomaten sind an den HUBs bereits in Betrieb. Und die Reisenden werden den Aufenthaltsort ihres Gepäcks künftig mittels Smartphone-App in Echtzeit verfolgen können. Auch Smart Glasses bieten durch den Einsatz von Augmented Reality völlig neue Möglichkeiten. Das Flugzeug wird zunehmend zum fliegenden Rechenzentrum und unsere Kunden erwarten Konnektivität – immer und überall. Im Oktober werden die ersten

Fotograf: Oliver Rösler für Lufthansa Deutschland

Fotograf: Dominik Mentzos für Lufthansa Deutschland

Lufthansa-Flugzeuge der Kurz- und Mittelstreckenflotte mit Breitband-Internet an Bord starten. Und es wird nicht mehr lange dauern bis Passagiere ihren eigenen Streaming-Dienst über das In-Flight-Entertainment-System an Bord nutzen oder mit ihrem Smartphone telefonieren können.

Die Digitalisierung verändert die Luftfahrt auf allen Ebenen. Es geht nicht mehr nur darum, mit dem Flugzeug von A nach B zu kommen, sondern um das gesamte Reiseerlebnis. Die Customer Journey – also das Reiseerlebnis von der Buchung bis zur Ankunft – wird durch die Digitalisierung insgesamt deutlich einfacher und bequemer, sowohl am Boden als auch in der Luft. Wir möchten die Passagiere auf der gesamten Reise begleiten – über mehrere Verkehrsträger hinweg. Auch am Zielort wollen wir die Kunden beraten und ihnen individuelle Angebote unterbreiten. Durch die Digitalisierung gilt es nicht nur das eigene Angebot zu managen, sondern auch das Dritter, beispielsweise von Hotels. Es geht darum, eine ganzheitliche Erfahrung auf unseren direkten Vertriebskanälen zu ermöglichen.

Welche Kernprozesse sind in der Luftfahrt ohne IT gar nicht mehr möglich?

Der Einsatz von IT durchdringt heute sämtliche Kernprozesse der Luftfahrt und beschleunigt die Abwicklung von Flugzeug- und Passagierabfertigung durch automatisierte Lösungen. Die meisten Prozesse würden heute gar nicht mehr ohne vollständige Digitalisierung funktionieren. Fast jede Schnittstelle zwischen uns und dem Fluggast ist elektronifiziert. Ohne IT-Unterstützung würde allein das Einsteigen in ein Flugzeug bis zu fünf Stunden dauern. Wir entwickeln kontinuierlich neue Lösungen, um die Kernprozesse bestmöglich zu steuern und weiter zu optimieren.

Big Data wird zunehmend zum Erfolgsfaktor, um Kunden zu binden und Umsätze zu steigern. Die Vielfalt an Daten wird analysiert, um wiederkehrende Muster zu identifizieren. Aus diesen wiederum lassen sich Vorhersagemodelle ableiten. Basierend auf den gewonnen Erkenntnissen über die Kundenbedürfnisse lassen sich Kundenservices verbessern und Verkaufsaktivitäten präzisieren.
Als Unternehmen sind wir nun in der Lage, weitaus fundiertere Entscheidungen zu treffen in welcher Art und Weise und über welche Themen mit dem Kunden kommuniziert wird.

Früher gab es nur den Premium- und Statuskunden, um den man sich personalisiert gekümmert hat.
Heute lernen wir unsere Kunden immer besser kennen und sind in der Lage, individualisierte Profile unserer Gäste zu erstellen. Wir können sie auf ihrer Reise individuell begleiten und ihnen ein auf ihre spezifischen Bedürfnisse und Vorlieben abgestimmtes Flugerlebnis ermöglichen. Wenn Sie fliegen, freuen Sie sich bestimmt auch über Ihr Lieblingsgetränk, Ihre Lieblingszeitschrift oder das Entertainmentprogramm Ihrer Wahl.

Die Digitalisierung erhöht zudem die Effizienz in der

Bild: Lufthansa Deutschland

Fotograf: Oliver Rösler für Lufthansa Deutschland

Luftfahrt, zum Beispiel durch eine schnellere Abfertigung von Passagieren und Gepäck am Flughafen. Zudem werden Flugzeuge künftig mittels digitaler Technologien eigenständig die effizientesten Routen wählen. Eine Software wertet hierzu die aktuellen Flugzeug- und Wetterdaten in Echtzeit aus. Das hilft, die Kosten in der Luftfahrt zu senken, denn eine effizientere Routenplanung macht sich unmittelbar im Kerosinverbrauch bemerkbar.
Eine genaue Vorhersage der Ankunftszeit ermöglicht es, auch die operativen Prozesse am Boden optimal auszurichten.

Wie wird sich die Rolle der IT bei der Lufthansa bis 2025 verändern?

Mit der digitalen Transformation ergeben sich ganz neue Anforderungen an die IT. Während in der Vergangenheit ein stabiler Betrieb der IT-Systeme zur Unterstützung der Geschäftsprozesse im Fokus stand, werden heute immer häufiger Fähigkeiten zum schnellen Erproben von Innovationen von der IT gefordert. Durch die Digitalisierung sind vormals IT-ferne Geschäftsmodelle zunehmend IT-getrieben. Digitale Lösungen entwickeln sich mehr und mehr zum Kerngeschäft. Neue, teils branchenfremde Wettbewerber treten in die eigenen Märkte ein, teilweise mit ganz neuen Geschäftsmodellen. Daten gewinnen eine immer größere Bedeutung – gleichzeitig muss die entstehende Informationsflut auch bewältigt werden.

Dadurch verändern sich auch grundlegend die Methoden und Prozesse der Produktentwicklung. Wir müssen heute in der Lage sein, neue Technologien auszuprobieren und Entwicklungen schnell vorantreiben, um schnell auf Kunden-Feedback und Marktentwicklungen zu reagieren, ohne Stabilität und Sicherheit aufzugeben. Um diese Anforderungen zu erfüllen, müssen wir nicht nur die IT-Landschaft umbauen, wir brauchen künftig in der IT zusätzliche Fähigkeiten und neue Arbeitsmodelle, um beispielsweise die Potenziale digitaler Interaktion mit Fluggästen, Mitarbeitern und Geschäftspartnern besser auszuschöpfen. Unternehmen müssen agiler und experimentierfreudiger werden. Sie dürfen keine Angst vor Fehlern haben, sollten Fehler zulassen, daraus lernen und die Erkenntnisse nutzen, um neue Geschäftsprozesse zu entwickeln. Das erfordert wesentlich mehr Flexibilität von uns, um Prototypen oder Proof of Concept schnell liefern zu können. Es ist ein kontinuierlicher Lernmodus, der auch von der IT unterstützt werden muss. Ein Paradigmenwechsel im Vergleich zum traditionellen Wasserfallmodell und langfristigen Ausschreibungen.

Die Prioritäten verschieben sich: Investitionen in IT sind heute genauso wichtig wie Investitionen in Flugzeuge. Die IT ist heute elementarer Bestandteil nahezu aller Produkte. Innovationen und neue Technologien sind von ausschlaggebender Bedeutung, wenn wir im globalen Kampf um Kunden bestehen und deren immer spezifischere Bedürfnisse befriedigen wollen.

Die IT wird zum Innovationsmotor und verschafft uns entscheidende Wettbewerbsvorteile. Deshalb muss die IT heute viel früher in Prozesse eingebunden werden, egal ob es um die Entwicklung neuer Produkte und Plattformen geht, die Planung der Launch-Strategie oder neue Preissysteme. Dabei gilt es, Bedürfnisse und Trends immer wieder aufs Neue zu identifizieren, aufzugreifen und die eigenen Angebote anzupassen. Um die IT-Welt enger mit der Unternehmensstrategie zu verknüpfen, berichte ich auch nicht mehr an den CFO, sondern direkt an den Lufthansa Vorstand für Hub-Management.

Welchen Stellenwert hat IT-Sicherheit heute und in 2025 bei der Lufthansa?

In einer immer stärker vernetzten Welt gewinnen nicht nur die Daten und der schnelle Zugriff darauf an Bedeutung, sondern vor allem deren Sicherheit. Cloud Computing, Big Data, Mobility und IoT sind derzeit die disruptiven Technologien, die in vielen Bereichen einen gewaltigen Wandel auslösen. Die zunehmende Interaktion mit Kunden, Mitarbeitern und Geschäftspartnern stellt uns vor neue Herausforderungen. Es entstehen neue Angriffsflächen, die es gilt geeignet abzusichern. Der Bedarf an technischen Sicherheitslösungen wird in den nächsten Jahren steigen. Kein Unternehmen kann sich Sicherheitslücken leisten.

Auch der Bereich Big Data ist extrem sensibel. Denn es werden persönliche Daten mit Wissen verknüpft, was ein hohes Maß an Datenschutz und -sicherheit erfordert. Das Mobile Business und das Internet der Dinge lassen den Datenverkehr ebenfalls stark anwachsen. Und die Bereitstellung von IT-Diensten wie Hardware, Software oder Plattformen durch Fremdanbieter über das Internet erfordert eine dedizierte Auseinandersetzung mit der Dienstleistung. Wie sieht konkret das Einsatzszenario aus? Welche Anforderungen muss der Anbieter erfüllen? Diese und andere Fragen müssen geklärt und neue Sicherheitskonzepte entwickelt werden.

Aber nicht nur von außen drohen Gefahren für die IT-Sicherheit, auch von innen, zum Beispiel durch den Datenzugriff unserer Crews über mobile Endgeräte. Daher müssen wir auch im Unternehmen für ein ausgeprägtes Sicherheitsbewusstsein sorgen und unsere Mitarbeiter entsprechend schulen. In den Flugzeugen gilt es zudem die Netzwerke für WLAN und Unterhaltungselektronik strikt von der sicherheitsrelevanten Technik an Bord zu trennen.

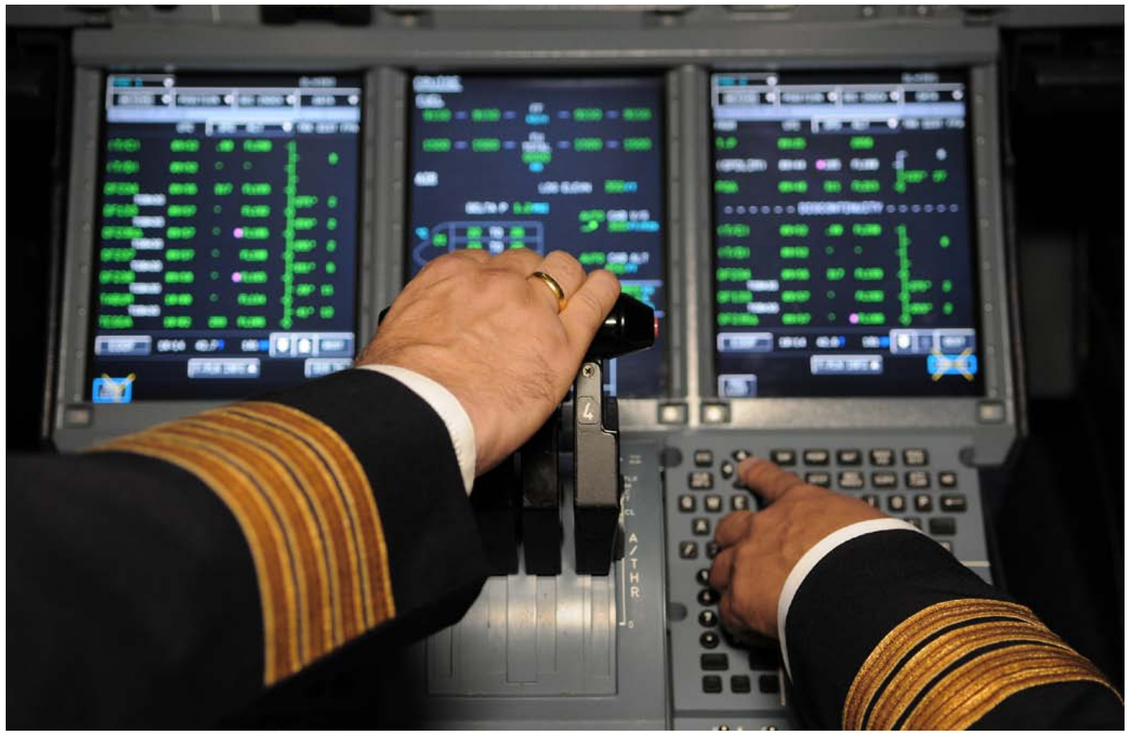


Bild: Lufthansa Deutschland

Cyberattacken und IT-Sicherheit in 2025

Die große **Expertenbefragung** zu den Zukunftstrends und -herausforderungen der IT-Sicherheit

IT-Sicherheitsexperten in Europa und Asien wurden gefragt: Wie entwickeln sich Cyberattacken bis 2025 und was müssen wir tun, um sie erfolgreich zu bekämpfen? Die Antworten geben klare Hinweise auf das, was auf Unternehmen und Nutzer zu kommt und auf die vielen Bereiche in denen es dringend etwas zu tun gibt.

iStock.com/hocus-focus

GEFAHR NR. 1:

die Zahl der Angriffe im Rahmen des Internet of Things explodieren

Das erwartet fast ein Viertel der Befragten. Nicht nur eine vergleichsweise leichte Angreifbarkeit der Geräte wird als Gefahr gesehen. Vielmehr wird das Internet of Things auch als Ausgangspunkt für einen Anstieg der Cyberkriminalität betrachtet.

„Das Internet der Dinge wird zukünftig eine wichtige Rolle spielen. Alles wird miteinander vernetzt sein. Wegen des Vorkommens verschiedener Standards nebeneinander wird es immense IT-Sicherheitsprobleme geben. Uralte Attacken kommen wieder auf – speziell bedingt durch das Internet der Dinge, weil sich dabei niemand um die IT-Sicherheit kümmert (und die meisten Geräte auch gar nicht in der Lage sind, ein hinreichendes IT-Sicherheitsniveau zu bieten).“ (Expertenkommentar im Wortlaut)

GEFAHR NR. 2:

Schadsoftware der nächsten Generation wird noch gefährlicher

Laut Experten entwickelt sich Schadsoftware in all ihren Facetten zukünftig wesentlich weiter.

„Kunden akzeptieren eingebaute Hintertüren in Standardsoftware . Diese Sicherheitslücken können herstellerseitig unzureichend gesichert sein und sind damit für Hacker ausnutzbar. Autonom agierende Computerprogramme werden Systeme attackieren und zwar mit bisher unbekannter Präzision, Reichweite und Geschwindigkeit.“ (Expertenkommentar)

GEFAHR NR. 3:

Der Nutzer als Startpunkt für Angriffe, allem voran bei Social Engineering Attacken

„Nutzer werden das schwächste Glied im gesamten System bleiben.“ (Expertenkommentar)

Nutzer werden heute und in der Zukunft als Startpunkt für gezielte als auch massenweise Attacken gesehen. Große Gefahr geht dabei besonders von Social Engineering Attacken aus. Angreifer spionieren das persönliche Umfeld ihres Opfers aus oder täuschen Identitäten vor. In 2016 wurden mehrere Fälle mit Schäden in zweistelliger Millionenhöhe bekannt.

Was sollen Unternehmen also tun, um fit für die Zukunft zu sein? Auch dazu haben die Experten klare Meinungen geäußert und damit strategische Handlungsempfehlungen zur Schaffung von mehr Sicherheit in der Unternehmens-IT gegeben.

Stärken Sie das Bewusstsein auf allen Hierarchieebenen und bilden Sie Ihre IT-Sicherheitsverantwortlichen laufend weiter

Der Mensch steht im Mittelpunkt der richtigen Ressourcenallokation, die die Experten für die Zukunft empfehlen. Auf ein fehlendes Bewusstsein für IT-Sicherheit auf allen Hierarchieebenen weist fast die Hälfte der Experten hin.

„Der Mangel an Fachkräften ist derzeit mit das größte Problem, das aber wirklich größte ist die Ignoranz auf CxO Ebene und das man IT-Security so lange nur als Kostenfaktor sieht bis wirklich etwas passiert. Das ist heute so und wird sich vielleicht bis 2025 ein wenig ändern.“ (Expertenkommentar)

Die neuen Technologien verstärken die Notwendigkeit, am Bewusstsein für IT-Sicherheit dringend anzusetzen.

„Cloud steht heute für die meisten Sicherheitsprobleme, aufgrund der notwendigen Kostenreduktionen in Unternehmen. Personen und Unternehmen kümmern sich immer noch nicht viel um IT-Sicherheit. In 2025 werden noch mehr wichtige Daten online sein, mehr Systeme werden verbunden sein und können mit sehr bösen Folgen manipuliert werden.“ (Expertenkommentar)

Richten Sie mehr Aufmerksamkeit auf die automatisierte Analyse sicherheitsrelevanter Daten in Echtzeit

Gleich nach den Investitionen in die „Ressource Mensch“ stehen Investitionen in den Fortschritt von IT-Sicherheitstechnologien.

Die Experten sehen allem voran die Notwendigkeit von Investitionen in die automatisierte Analyse sicherheitsrelevanter Daten in Echtzeit. Auch die Verschmelzung von IT die in Produkten steckt und deren IT-Sicherheit ist ein mehrfach adressiertes Thema. Das heißt: IT-Sicherheit schon bei der Produktentwicklung mitbedenken.

„(Geschafft werden sollte…) ein besserer Gesamtzugang zum Thema IT-Sicherheit: Attacken voraussagen und Sicherheitsmechanismen in den Applikationen selbst implementieren, nicht nur in der Sicherheitsebene darüber.“ (Expertenkommentar)

Fördern und gestalten Sie die IT-Sicherheitsforschung mit und ziehen Sie Ihren Nutzen daraus

Die Forschung zum Einsatz von künstlicher Intelligenz und automatisierten Angriffserkennungsverfahren sind die wichtigsten Ansätze für die IT-Sicherheitstechnologie der Zukunft. Bahnbrechende Entwicklungen sind bis 2025 zu erwarten. Auch neue Authentifizierungsverfahren bilden zukünftig entscheidende Sicherheitsmechanismen. Ob Cyberangreifer oder IT-Sicherheitsverantwortliche das Wettrennen gewinnen, entscheidet sich vor allem durch den jeweiligen Fortschritt bei der Technologie.

„IT-Security Systeme könnten untereinander besser kommunizieren und sich gegenseitig tunen (Selbstverteidigung der Systeme). Ob dies im Rahmen von Künstlicher Intelligenz 2025 möglich sein wird, ist fraglich.“ (Expertenkommentar)

Lesen Sie die gesamte Studie hier:
www.radarservices.com/de/2025/

Organisierte Cyberkriminalität

Die 3 „Must-haves“ für die zeitnahe Erkennung von gezielten Cyberangriffen

Gezielte Cyberangriffe verursachen den höchsten Schaden, wenn sie von IT-Sicherheitsbereichen über längere Zeit unentdeckt bleiben. Angreifer spionieren ungestört das Netzwerk aus bis sie schlussendlich die Kronjuwelen des Unternehmens finden – und entwenden.

Schutz vor solchen besonders gefährlichen Angriffen bietet ein kontinuierliches IT Security Monitoring. Seine Aufgabe: Die zeitnahe Erkennung von Cyberangriffen aus allen Risikobereichen der Unternehmens-IT. Die Technologie dazu umfasst drei zentrale Komponenten.

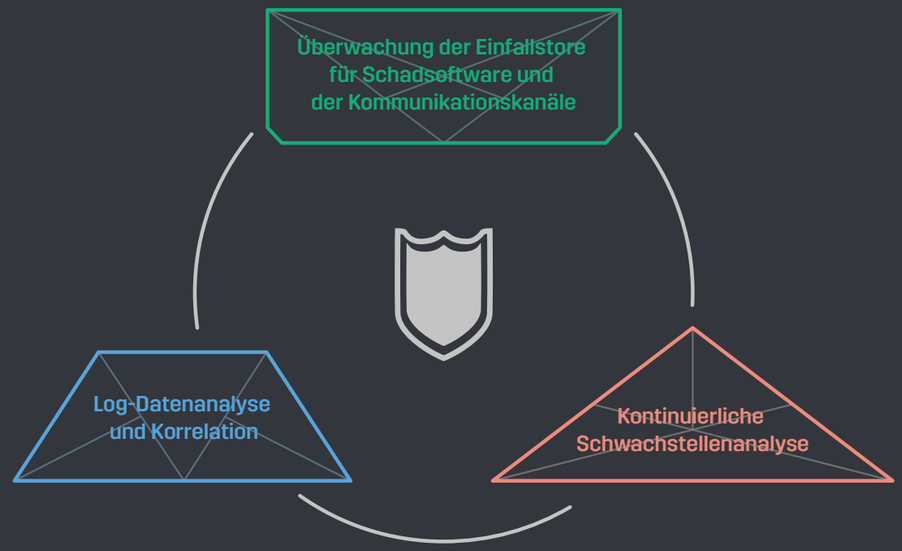
Die Überwachung der Einfallstore für Schadsoftware und der Kommunikationskanäle

Öffentliche Institutionen sind von Datendiebstahl genauso betroffen wie Unternehmen. So entwendeten Cyberangreifer vor wenigen Monaten Daten von 4 Millionen US-Regierungsangestellten bei deren Personalstelle, 83 Millionen Kundendaten bei J.P. Morgan Chase und 80 Millionen beim Versicherer Anthem. Fakt ist aus Techniksicht: Ein Angreifer muss die Daten früher oder später aus dem Unternehmen zu externen Zielen im Internet übertragen. Das fällt beim Security Monitoring aller Systeme, des Datenverkehrs und der Zugriffe auf sensible Systeme und Dateien auf. Datentransfer von internen zu externen IPs, zu denen keine Geschäftsbeziehung besteht, muss umgehend festgestellt und analysiert werden. Hier setzen unter anderem Intrusion Detection Systeme (IDS) an. Sie zeichnen den Fluss von Datenpaketen auf, analysieren sie und melden verdächtige Aktivitäten.

Ein anderes Einfallstor: Schadsoftware in Email-Attachments oder Web Downloads. Immer wieder sind zum Beispiel deutsche Großkrankenhäuser im Feuer der Ransomware. Die Erpressungssoftware sperrt Computer oder verschlüsselt Teile der Festplatte. Nur nach Zahlung des Lösegelds erfolgt eine Entschlüsselung. Aus Sicherheitsgründen arbeiteten alle betroffenen Kliniken über Tage hinweg offline und „im Handbetrieb“. Dabei hätten die Betriebsstörungen vollständig vermieden werden können: Beim Einsatz der neuesten Generation von „Sandboxing“-Technologien werden alle eingehenden E-Mails und alle Downloads von Mitarbeitern aus dem Internet automatisiert in „abgeschotteten“ Umgebungen („Sandboxen“) analysiert. Wird eine Schadsoftware entdeckt, wird das Email aufgehalten oder der Web-Download gestoppt. Damit ist auch der Cyberangriff erfolgreich abgewehrt.

Die kontinuierliche Schwachstellenanalyse

Jeden Tag entstehen neue Angriffsarten, die bisher unbekannte Sicherheitslücken oder Schwachstellen in der IT eines Unternehmens ausnutzen. So wurde 1blu, eines der größten, deutschen Webhosting-Unternehmen nach eigenen Angaben Opfer einer umfassenden Datenentwendung und eines Erpressungsversuchs. Der Zugriff auf das interne 1blu-System erfolgte über eine fehlerhafte Serverkonfiguration, die dem Angreifer ein sukzessives Ausspähen der mehrstufigen Systemarchitektur ermöglichte. Zwar wurden die Daten zum Großteil verschlüsselt gespeichert, die Verschlüsselung konnte jedoch offensichtlich vom Angreifer entschlüsselt werden. Erleichtert wurde der Zugriff dadurch, dass die internen Vorgaben zur Sicherheit von Keys und Passwörtern von einzelnen Mitarbeitern nicht eingehalten wurden.



Das kontinuierliche Aufspüren von fehlerhaften Konfigurationen und Sicherheitslücken mittels Schwachstellenscanner aus einer internen Sicht (innerhalb des Unternehmensnetzwerkes) und aus einer externen (aus dem Internet) ist Voraussetzung für eine sichere IT. Die konsequente und nachvollziehbare Behebung im Rahmen des Schwachstellenmanagements schließt Einfallstore für Angreifer und verkleinert so ihren Aktionsspielraum.

Die Log-Datenanalyse und Korrelation

Der Deutsche Bundestag wurde in 2015 Ziel einer Cyberattacke. Nach Berichten waren Angreifer waren über einen Abgeordnetenrechner in das Netz eingebrochen. Sie haben sich Zugang zu Passwörtern von Administratoren verschafft und waren damit in der Lage auf Server zuzugreifen.

Dann versuchen sie ihre Bewegungen im Netzwerk so normal wie möglich aussehen zu lassen. Dennoch können diese Angreifer entdeckt werden: Logins von einem Benutzer auf mehreren Systemen von unterschiedlichen IPs zur gleichen Zeit sind Hinweise. Alle Logs von Servern, Netzwerkgeräten, Applikationen und anderen Einrichtungen mit sicherheitsrelevanten Informationen müssen daher zentral analysiert und mit den Erkenntnissen aus den Intrusion Detection Systemen korreliert werden.

Dazu dient ein Security Information & Event Management (SIEM) in dem automatisiert alle Logs normalisiert, analysiert und mittels sogenannter Use Cases auf Sicherheitsvorfälle und Risiken hin untersucht werden.

Eine Advanced Correlation Engine mit ihren Erkennungsalgorithmen auf Basis von Regeln und statistischen Modellen ermöglicht die Umsetzung dieser Use Cases und ihre laufende Überprüfung, auch in Kombination mit Schwachstelleninformationen und Analysen des Netzwerkdatenverkehrs.

Conclusio

Unternehmen sind gut gewappnet, wenn sie moderne Technologien in allen drei Bereichen im Einsatz haben. Aber Vorsicht – Werkzeuge sind schlussendlich immer nur so gut wie ihre Anwender: Die korrekte Konfiguration und Anpassung an aktuelle Gegebenheiten ist eine zentrale und laufende Aufgabe für hochspezialisierte Experten.

Mensch versus Maschine

Wie selbstlernende Systeme Cyberangriffe erkennen

Selbstlernende Systeme werden derzeit in vielen Bereichen erprobt. Eines der spannendsten Themen: Die Aufdeckung von Cyberangriffen. Die Forschung ist weit fortgeschritten, der Praxistest erfolgt. Nun wird an den Feinheiten getüftelt. Im Interview: Harald Reisinger, Geschäftsführer von RadarServices, dem in der Erforschung des Themas führenden Unternehmen in Europa.

iStock.com/ktsimage

Machine Learning wendet Algorithmen an, um Muster oder Beziehungen in bestehenden Daten zu erkennen. Zugrunde liegen verschiedene statistische Methoden, unter anderem die klassische Inferenzstatistik, Bayesche Modelle oder Clustering. Auf dieser Basis werden von den als „selbstlernend" oder auch als „verhaltensbasiert" bezeichneten Systemen automatisiert Schlüsse gezogen, Wahrscheinlichkeiten für verschiedene Szenarien berechnet und Vorhersagen getroffen.

Solche verhaltensbasierten Systeme werden zum Aufdecken von Cyberangriffen in der IT-Infrastruktur von Unternehmen und öffentlichen Institutionen eingesetzt. Dazu Harald Reisinger: *„Herkömmliche IT-Sicherheitswerkzeuge sind üblicherweise regel- bzw. signaturbasiert. Das heißt, dass sie zum Beispiel Schadsoftware nur dann erkennen, wenn ihnen vorab exakte Informationen über deren Eigenschaften zur Verfügung standen. Bei geringsten Abweichungen von diesen Vorgaben werden die Werkzeuge überlistet und sind wirkungslos. Angreifer konzentrieren sich genau darauf: Sie finden und nutzen neuartige Schwachstellen in der Infrastruktur eines Unternehmens aus oder setzen bisher unbekannte Schadsoftware ein. Heute braucht es Spezialisten, um solche Angriffe zu erkennen. Erst Machine Learning kann die menschliche Analysefähigkeit mit ihren logischen Schlussfolgerungen sukzessive ersetzen."*

Ein Beispiel aus der IT-Sicherheitspraxis

Aus einem Firmennetzwerk werden Daten gestohlen, im Fachjargon wird dieser Vorgang „Data Exfiltration" genannt. Ein signaturbasiertes System erkennt möglicherweise ein bestimmtes URL-Muster für Uploads zu einer potenziell gefährlichen Webseite oder es identifiziert eine bereits bekannte Schadsoftware. Geübte Angreifer können dies aber leicht umgehen. Verhaltensbasierte Systeme erkennen hingegen, dass gerade ein Dateiupload stattfindet. Zusätzlich sind sie in der Lage zu melden, wenn dies von einem Rechner aus geschieht, der selten Dateiuploads ausführt oder wenn die Zieladresse unüblich ist. Einem Angreifer wird es sehr schwer fallen, das zentrale Ziel seines Angriffs, den Dateiupload, zu verschleiern.

Der Status Quo der Forschung und Anwendung

Machine Learning wurde in der Forschung zwar erstmals 1999 erwähnt, war aber in der Praxis aufgrund der immens langen Rechenzeit und den dafür notwendigen, hochleistungsfähigen Prozessoren über Jahre hinweg kaum angekommen. Heute sind die technischen Voraussetzungen vorhanden und das Thema ist eines der vielversprechendsten Ansatzpunkte, um Arbeitsschritte, die derzeit IT-Sicherheitsexperten „manuell" ausführen, zu automatisieren.

Der Erfolg in der Anwendung hängt dabei sehr stark von der Qualität der Datenbasis ab. Das ist nicht speziell ein Problem für den Bereich IT-Sicherheit, sondern ein generelles statistisches Problem. Reisinger: *„Während Ereignisse mit sehr hoher Signifikanz automatisiert leicht zu erkennen sind, besteht die Kunst darin, automatisiert Ereignisse mit niedriger Signifikanz in ‚für die IT-Sicherheit wichtiges' und ‚unwichtiges' zu unterscheiden. Dafür hat sich in der Praxis noch kein Modell durchgesetzt. Hier liegt daher auch der Forschungsfokus für die Weiterentwicklung unserer verhaltensbasierten Systeme. Reichert man deren Informationen mit Erkenntnissen aus anderen Datenquellen wie signaturbasierten Systemen an, erhält man qualitativ sehr hochwertige Daten über Auffälligkeiten in einem Unternehmensnetzwerk. Mit ihnen wird die automatisierte Beurteilung der Relevanz eines Ereignisses im Unternehmensnetzwerk als tatsächlicher Sicherheitsvorfall möglich."*

Um Machine Learning weiterzuentwickeln, werden bei RadarServices auch Technologien aus anderen Branchen und Geschäftsfeldern wie der Ökonometrie oder der Bioinformatik auf Analogien untersucht. Auf dieser Basis erfolgt schrittweise ein immer weitergehender Praxiseinsatz für Maschinen, die menschliche Fähigkeiten erlernen und intelligent einsetzen können.

iStock.com/vasilypetkov

IT-Sicherheit wird durch den Einsatz von spezialisierter Software erreicht – so das in der Allgemeinheit vorherrschende Bild. Doch in Großunternehmen und öffentlichen Institutionen wird viel mehr getan, um Kundendaten, Betriebsgeheimnisse und interne Kommunikation tagtäglich vor Cyberangriffen zu schützen. Im Mittelpunkt steht das Security Operations Center (SOC).

Sicher wie Fort Knox?

Warum selbst fortschrittlichste Institutionen anfällig für Cyberangriffe sind

DAS Security Operations Center (SOC) ist mit einem Tower am Flughafen vergleichbar. Basierend auf modernster Technologie beobachten und beurteilen Experten permanent die aktuelle IT-Sicherheitslage in der gesamten IT-Landschaft einer Organisation und ergreifen bei Auffälligkeiten sofort die richtigen Gegenmaßnahmen.

J.P. Morgan, Sony Playstation Network, Adobe Systems, Ebay, Oracle, Deutscher Bundestag oder Democratic Congressional Campaign Committee (DCCC) im US-Wahlkampf: Dass Cyberangreifer trotzdem bei den fortschrittlichsten Unternehmen und Institutionen der Welt immer wieder erfolgreich sind, zeigt, dass eine detaillierte Sicherheitsüberwachung offenbar nicht immer einwandfrei funktioniert.

Wo liegen die häufigsten Probleme? Eine Analyse gibt Einblick und gleichzeitig Tipps für das Set-Up von Sicherheitsbereichen in großen Organisationen.

PROBLEM 1:

Es gibt kein dezidiertes SOC

Beispiel: Großkrankenhäuser. 2016 wurden mehrere Fälle von Ransomware-Angriffen vor allem in Deutschland, den USA und Kanada bekannt. Die Erpressungssoftware legte die IT und damit die Prozesse der Organisationen über Tage lahm. Trotz fortschrittlichster Medizintechnik scheinen im Bereich IT-Sicherheit wichtige Maßnahmen zu fehlen, die derartige Angriffe von vorneherein unschädlich gemacht hätten.

Geschätzte 85% aller deutschen Unternehmen mit mehr als 1.000 Mitarbeitern verfügen aktuell über kein dezidiertes SOC. Dabei ist die Einrichtung eines SOCs für große Organisationen ein Muss. Denn die Millionenschäden und die negativen Reputationsfolgen kommen bei Cyberangriffen immer dann zustande, wenn eine Organisation über keine geeigneten technischen Werkzeuge und Experten verfügt und so über Wochen oder Monate hinweg nicht erkennt, dass es angegriffen wird. In diesem Fall haben Angreifer genügend Zeit, das schwächste Glied im gesamten Unternehmensnetzwerk ausfindig zu machen. Sie können zum Beispiel über Mitarbeiter-Accounts Schadsoftware einspielen oder massenweise Daten entwenden. Ohne ein dezidiertes SOC werden solche „Vorbereitungsarbeiten“ von Hackern oftmals nicht festgestellt.

PROBLEM 2:

Installation von Security Software alleine reicht nicht

Für die IT-Risikoerkennung sind eine Reihe von komplexen Systemen, Software und Informationsquellen notwendig. Dazu gehören zum Beispiel Schwachstellenscanner, Intrusion Detection Systeme, ein Security Information & Event Management System, Sandboxing-Technologien, Threat Intelligence und Reputationsdaten sowie Correlation Engines. Mit dem Kauf dieser Produkte ist es aber nicht getan. Experten müssen sie laufend konfigurieren und an die aktuellen Gegebenheiten im und um das Unternehmen anpassen, damit sie einen Angriff auch richtig und rechtzeitig erkennen. Auch sind die Erkenntnisse der Software lediglich Risikohinweise. Experten müssen die Informationen also analysieren, hinsichtlich ihrer Gefahr bewerten, ihre Auswirkungen auf die IT und die Geschäftsabläufe hinterfragen, für die Behebung priorisieren, für die operativen IT-Teams mit Behebungshinweisen versehen und schlussendlich als „behoben“ klassifizierte Vorkommnisse einer Endkontrolle unterziehen.

Die Experten im SOC sind also nicht nur die entscheidenden Alarmgeber bei Cyberangriffen. Sie koordinieren vor allem auch die Aufgaben der operativen IT-Teams wenn rasche Reaktionen auf Angriffe notwendig sind, um damit eine größtmögliche Schadensbegrenzung zu erreichen. Sie machen das SOC zur Schaltzentrale für ein effektives IT-Risikomanagement.

PROBLEM 3:

Funktionierende Prozesse fehlen

Der Cyberangriff auf die US-Handelskette Target in 2013 demonstrierte die Folgen von nicht-funktionierenden Prozessen besonders plakativ: Mehr als 100 Millionen Datensätze von Kunden wurden entwendet. Berichten zufolge war das Unternehmen durch seinen IT-Sicherheitsdienstleister über Auffälligkeiten im Netzwerk rechtzeitig informiert, die zeitnahe Reaktion darauf blieb jedoch aus.

Die teuerste Software und ein geschultes Expertenteam helfen also nicht, wenn Prozesse nicht etabliert sind und gelebt werden. Im akuten Angriffsfall sind gut funktionierende Workflows innerhalb des SOC-Teams sowie zwischen diesem und den operativen IT-Teams das A und O. Die zuständigen Mitarbeiter müssen in einem regelmäßigen, persönlichen Austausch stehen, damit sie im Notfall sofort Hand in Hand miteinander arbeiten können.

FAZIT

Cyberangriffe stellen auch für die fortschrittlichsten Organisationen der Welt eine Herausforderung dar. Die Erfolgsformel besteht aus drei Komponenten: modernsten Werkzeugen, geschulten Experten und etablierten Prozessen. Wird dies erfüllt, sind auch große und besonders im Fadenkreuz von Angriffen stehende Institutionen sicher. IT-Sicherheit ist dabei ein laufender Prozess, kein Einmalinvestment.

Datenübertragung in die USA: IT-Sicherheit darf sich auch im Cloud-Zeitalter nicht in Luft auflösen

DAS DATENSCHUTZNIVEAU zwischen den USA und Europa ist unterschiedlich – das bestätigte der Europäische Gerichtshof. Er kippte das „Safe Harbor"-Abkommen, die bis dahin am häufigsten genutzte rechtliche Grundlage für den Transfer personenbezogener Daten zwischen den USA und der EU. Das „EU-US Privacy Shield", Nachfolger von „Safe Harbor", wird von Europas Datenschützern ebenso kritisch gesehen. So begründet sich eine rechtlich schwierige Situation und namhafte Unternehmen mussten bereits Strafen zahlen, da sie Datentransfers weiterhin auf „Safe Harbor" stützen.

Neben personenbezogenen Daten übertragen europäische Unternehmen aber auch – und noch immer legal – hochsensible Daten über ihre tagesaktuelle IT-Sicherheit an meist cloud-basierte Dienstleister in den USA. Die Datenschutzbedenken von Experten sind dabei immens.

So werden beispielsweise laufend Daten über den tagesaktuellen Stand der IT-Sicherheit von Unternehmen zu Analysezwecken in die USA übertragen. Dieses IT Security Monitoring verarbeitet Logs, sicherheitsrelevante Ereignisse und Informationen über Schwachstellen aus der IT-Infrastruktur. Die Informationen werden von externen Systemen bewertet und – falls auffällig – von dortigen Experten untersucht. Während dadurch mögliche Cyberangriffe erkannt und so die IT-Sicherheit erhöht werden sollen, wird eine neue Gefahr geschaffen, denn: Verlassen die Daten einmal ein Unternehmen und darüber hinaus Europa, sind sie ebenso wenig vor dem Zugriff und der Weiterverwendung durch US-Behörden geschützt wie es personenbezogene Daten sind.

Das gilt auch wenn die Analysezentren der US-Sicherheitsdienstleister in Europa angesiedelt sind – auch hier ist ein Zugriff durch US-Behörden aufgrund des Patriot Act jederzeit möglich.

Dringend empfehlenswert ist daher eine europäisch geprägte Herangehensweise für sicherheitsrelevante Daten. Ein „Anti-Cloud Prinzip" für die IT-Security. Das oberste Prinzip: Diese Daten dürfen niemals über die eigenen Unternehmensgrenzen hinweg übertragen werden.

Erhöhte Kosten für die IT-Sicherheit entstehen dadurch nicht. Haben Unternehmen keine ausreichend großen, eigenen IT-Sicherheitsbereiche, können sie weiterhin mit externen Dienstleistern zusammenarbeiten. Der heutige Stand der Technik erlaubt die Erbringung sämtlicher Services auch ohne Datenübertragung über Unternehmensgrenzen hinweg.

News, Events und Infos aus dem Hause RadarServices

Über uns

RadarServices ist Europas führender Anbieter von Managed Security Services. Im Mittelpunkt steht die zeitnahe Erkennung von IT-Sicherheitsrisiken. Daten verlassen dabei niemals ein Kundenunternehmen. Die Services kombinieren (1) die zu 100% in Europa entwickelte Technologie, (2) die Arbeit der Analyseexperten in den weltweiten Security Operations Centers (SOCs) und (3) bewährte Prozesse und Best Practices bei IT-Sicherheitsvorfällen. Das Ergebnis: Eine besonders effektive und effiziente Verbesserung von IT-Sicherheit und Risikomanagement, ein kontinuierliches IT Security Monitoring und ein auf Knopfdruck verfügbarer Überblick über die sicherheitsrelevanten Informationen im Gesamtunternehmen.

RadarServices hat seinen Hauptsitz in Wien, Österreich. Zu den Kunden gehören mittelständische und große Unternehmen mit bis zu 350.000 Mitarbeitern sowie Behörden.

Mit unseren weltweiten SOCs wird eine Serviceerbringung in Ihrer Nähe gewährleistet.

Neue E-Books für den Auf- und Ausbau Ihres Cyber Defence Centres

Was ist ein Security Operations Centre (SOC) und was ist es nicht?
Wie wird ein SOC in einem Unternehmen oder Behörde aufgebaut und was kostet dessen Betrieb?
Managed SOC als Alternative zum Eigenbetrieb – wie wählt man einen externen SOC-Dienstleister aus?

Diese Fragen werden anhand von konkreten Beispielen und Zahlen in den beiden **neuen Leitfäden** Eigenbetrieb eines SOCs versus SOC as a Service und SOC as a Service – Entscheidungskriterien für die Anbieterauswahl beantwortet.

Ein Jahr Cybersecurity World in Wien

3D Cybersecurity Modell jetzt auch im Pocket Format erhältlich

Vor einem Jahr, im Dezember 2016, eröffnete RadarServices die **Cybersecurity World in Wien**. An diesem weltweit einzigartigen Ort wird seitdem **IT-Sicherheit erlebbar**. Hier befindet sich das größte Cyber Defence Centre Europas. Und hier werden die heutigen und zukünftigen Herausforderungen für IT-Sicherheitsverantwortliche in Unternehmen und der aktuelle Stand von Research und Innovation in der Branche auf 2.000 qm illustriert.

Besucher unserer Headquarters erleben in **monatlich stattfindenden Führungen** „IT-Sicherheit zum Anfassen“: International ausgezeichnete Sicherheitsexperten geben Einblicke in ihre Arbeit und präsentieren Cyberattacken und Technologien für die IT-Risikoerkennung mit einem Cybersecurity Modell aus dem 3D-Drucker. Die Termine der Führungen und die Anmeldemöglichkeit finden Sie immer aktuell hier: https://www.cybersecurityworld.org.

Zum ersten Geburtstag gibt es die **Cybersecurity World nun auch im Pocket Format**: mit dem C**ybersecurity World GAME aus dem 3D-Drucker** können Angriffsszenarien auf eine Unternehmensumgebung simuliert werden. Mit roten Spielfiguren wird ein Angriff dargestellt, mit grünen Figuren folgt darauf die Präsentation der IT-Sicherheitsmaßnahmen, die den Angreifer in wenigen Sekunden entlarvt und seine Reise durch das Netzwerk des Opfers gestoppt hätten.

Das Cybersecurity World GAME wurde vor kurzem in London mit dem „AOA Annual Award 2017“ ausgezeichnet. Es wird in den Größen 120cm × 120cm und 80cm × 80cm auf **Messen, Konferenzen und Veranstaltungen** und in der Größe 30cm × 30cm (Brettspielgröße) bei **Awareness Trainings und internen Präsentationen** in Unternehmen eingesetzt und sorgt bei den Zuschauern für ein Erlebnis, das im Gedächtnis bleibt.

Sie haben Interesse, ein Cybersecurity World Game zu erwerben? Kontaktieren Sie uns dazu gerne telefonisch oder per Email. Ihre Ansprechpartnerin bei RadarServices ist Isabell Claus (+43 1 9291271-777, news@radarservices.com).

CYBERSECURITY WORLD

RadarServices gibt Gas

Bei RadarServices arbeiten interessante Menschen mit interessanten Hobbies. Partnermanager Wolfgang Wimmer ist Rallyefahrer. In 2016 fuhr er zum ersten Mal für das „RadarServices Rallye Team“. Sein Erfolg: Bei der Niederbayern Rallye wurde er mit durchschnittlich 103 km/h Dritter in der Klasse M1 für serienahe Fahrzeuge. Gewinner der Gesamtrallye wurde der amtierende Deutsche Meister Ruben Zeltner mit seinem Porsche 997 GT3. Es war eine Hitzeschlacht bei 34 Grad im Schatten. Bei der 97 km langen Strecke handelt es sich um eine der schnellsten Rallyes in Europa.

Gold

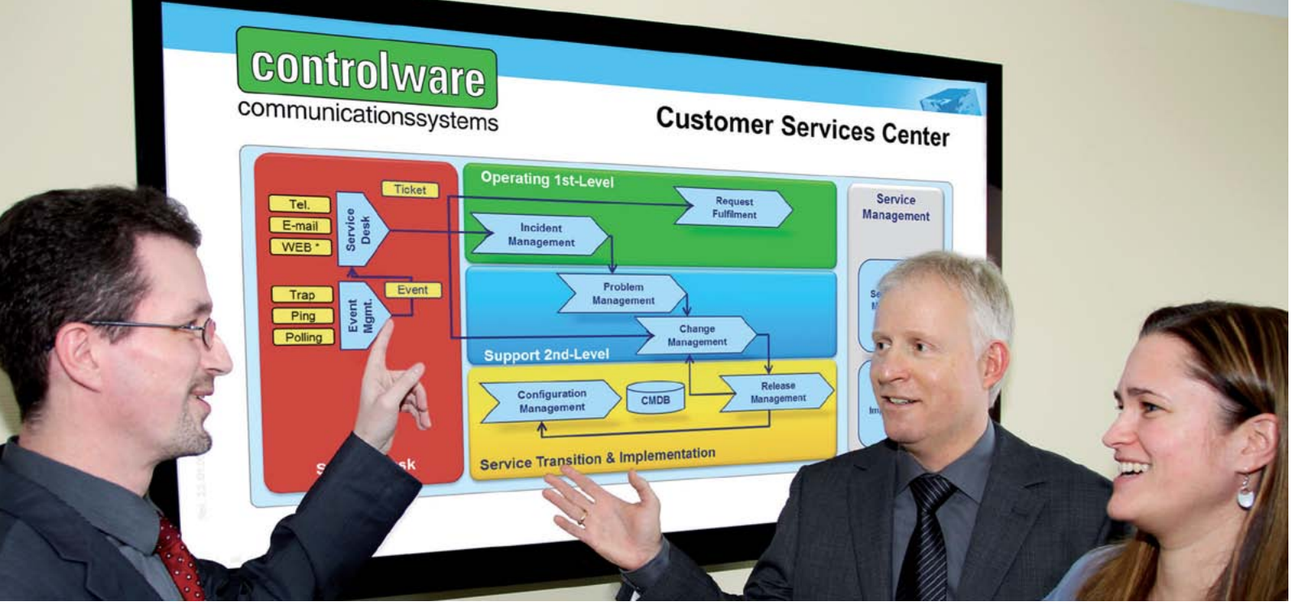
in der Kategorie „IT-Sicherheit“ für RadarServices Intelligence Team Mitglied

Die weltweit führende Aus- und Weiterbildungsorganisation für IT-Sicherheit, das SANS Institute, verleiht besonders talentierten und zur Weiterentwicklung der digitalen Forensik beitragenden IT-Sicherheitsspezialisten regelmäßig die „SANS Lethal Forensicator Coin“. Die mit der Medaille ausgezeichneten „Lethal Forensicators“ haben gezeigt, dass sie auch komplexeste Bedrohungen erkennen und beseitigen können und erstklassige Ergebnisse im Rahmen ihrer Aus- und Weiterbildung erzielen. Sie gehören zu den weltweit führenden Spezialisten in der Verteidigung von Organisationen während eines Cyberangriffs oder bei komplexen digitalen Untersuchungen. Die Auszeichnung kommt also einer Art „Goldmedaille für IT Security Fachleute“ gleich.

Einem Mitglied des RadarServices Intelligence Teams wurde die „SANS Lethal Forensicator Coin“ nun verliehen.

„Wir sind stolz auf unser Security Intelligence Team. Diese Spezialisten bilden sich nicht nur selbst kontinuierlich weiter, sondern tragen auch zur Weiterentwicklung der weltweiten Community bei. In den Bereichen digitale Forensik und Incident Response sind sie unschlagbar – das belegt nun auch die Verleihung der ‚SANS Lethal Forensicator Coin‘ an unser Teammitglied“ kommentiert Christian Polster, CFO & CSO von RadarServices.

Das SANS Institute wurde 1989 als Research- und Ausbildungsorganisation gegründet. Weltweit partizipierten mehr als 165.000 IT Security Fachleute in den Programmen, unter ihnen IT-Sicherheitsverantwortliche in globalen Organisationen der Privatwirtschaft und öffentlichen Hand.



Controlware – Ihr IT-Partner

Als erfahrener IT-Dienstleister verfügt Controlware über umfassendes Know-how in den Bereichen Network Solutions, Unified Communications, Information Security, Application Delivery, Data Center & Cloud sowie IT-Management.

Wir unterstützen Sie rund um die IT – von der Planung und Implementierung konvergenter Infrastrukturen bis hin zum Betrieb auf Basis ITIL-konformer Serviceprozesse.

Unser ISO-27001-zertifiziertes Customer Services Center bietet Ihnen individuell angepasste Managed Services, erweitert um umfassende Security Operating Services. Gemeinsam mit unserem Partner RadarServices haben wir für unsere Kunden aus dem Bereich der kritischen Infrastrukturen (KRITIS) eine innovative Managed IT-Security-Lösung entwickelt. Diese bietet umfassende Risikoerkennung über Logdaten-, Schwachstellen- und Datenstrom-Analyse in Verbindung mit bedarfsgerechter Reaktion auf Sicherheitsvorfälle. Darüber hinaus unterstützt die Lösung alle gängigen Industrieprotokolle der Versorger und unterliegt den EU-Datenbestimmungen. Besonders wichtig – alle Daten verbleiben beim Kunden.

Managed Security Services mit Controlware & RadarServices!

controlware
communicationssystems

Wir sind für Sie da!

Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel.: +49 6074 858-00
info@controlware.de
www.controlware.de

Treffen Sie unsere Experten

Persönlicher Kontakt ist uns sehr wichtig. Wenn es um IT-Sicherheit geht, müssen Sie Ihre Partner kennen und Ihnen vertrauen. Deshalb steht Ihnen das Team von RadarServices jederzeit für Vier-Augen-Gespräche zur Verfügung. Darüber hinaus treffen Sie uns auf Veranstaltungen unserer Vertriebspartner und Messen zum Thema IT-Sicherheit. In 2018 sind wir unter anderem auf der Münchner Cyber Security Konferenz 2018 (15.02.2018, München), dem Cybersicherheits-Gipfel Hessen 2018 (08.05.2018, Wiesbaden), infosecurity 2018 (05.-07.06.2018, London), it-sa 2018 (09-11.10.2018, Nürnberg) und der IKT-Sicherheitskonferenz 2018 (16.-17.10.2018, Alpbach).

Wichtige Termine

15.02.2018, München
Münchner Cyber Security Konferenz 2018

08.05.2018, Wiesbaden
Cybersicherheits-Gipfel Hessen 2018

05.–07.06.2018, London
infosecurity 2018

09.–11.10.2018, Nürnberg
it-sa 2018

16.–17.10.2018, Alpbach
IKT-Sicherheitskonferenz 2018

Impressum

RADAR SERVICES Publishing

Über RadarServices Publishing

RadarServices Publishing veröffentlicht Artikel, Berichte, Studien und Zeitschriften rund um das Thema IT-Sicherheit. Unser Ziel ist es, Einblick in die Erfahrung von Branchenexperten zu geben und Knowhow zum Thema IT-Sicherheit durch universitäres und nicht-universitäres Research an Unternehmen, öffentliche Institutionen und andere Organisationen weiterzugeben. Wir beziehen Co-Autoren aus Akademia und Wirtschaft aktiv ein um das Wissen über aktuelle Entwicklungen im Bereich IT-Sicherheit in der Öffentlichkeit und im Speziellen bei Führungskräften in Unternehmen sowie in der Politik zu fördern. RadarServices Publishing ist Teil von RadarServices.

Über diese Veröffentlichung

Diese Veröffentlichung beinhaltet ausschließlich generelle Informationen. RadarServices und/oder dessen verbundene Gesellschaften erbringen mit dieser Veröffentlichung keine fachliche Beratungsleistung. Diese Veröffentlichung ersetzt auch keine derartige Beratungsleistung und sollte auch nicht als Grundlage für Geschäfts- oder Investitionsentscheidungen/-handlungen verwendet werden. Weder RadarServices noch dessen verbundene Gesellschaften haften für Verluste, die eine Person im Verlassen auf diese Veröffentlichung erleidet.

Über RadarServices

RadarServices ist Europas führender Anbieter für kontinuierliches und vorausschauendes IT Security Monitoring und IT Risk Detection als Managed Services. Die Services kombinieren die automatisierte Erkennung von IT-Sicherheitsproblemen und -risiken mit der Analyse durch Experten. Daten verlassen dabei niemals das Kundenunternehmen. Für die Einrichtung, Konfiguration und den täglichen Betrieb sind keine zusätzlichen personellen oder finanziellen Ressourcen notwendig.

Adresse:
Cybersecurity World
Zieglergasse 6, 1070 Wien
Tel. +43 1 9291271-0
publishing@radarservices.com

Gesamtverantwortlich und Redaktion: Dr. Isabell Claus T.: 0043 1 9291271-33
Grafische Umsetzung: Thomas Fadrus
Fotos/Bildrechte: Deutsche Lufthansa; istockphoto.com; Coverbild: iStock.com/shulz


RADAR
SERVICES
Die nächste
Welle kommt.
SOC as a Service,
IT Security Monitoring,
Security Information & Event Management (SIEM),
Advanced Cyber Threat Detection und
IT Risk Detection
als Managed Services der nächsten Generation
Das Frühwarnsystem für Ihre IT.