itsecurity
MAI | JUNI 2018

DAS SPEZIAL

IT-SICHERHEIT

DIGITALISIERUNG, IOT & CYBERSECURITY

Detlev Henze, Geschäftsführer, TÜV Trust IT

SELBSTLERNENDE IT-SECURITY

Verteidigungsmechanismen suchen in Echtzeit nach Anomalien

BROWSER IN QUARANTÄNE

Dank „Virtualisierung" werden Sicherheitslücken geschlossen

MACHINE LEARNING

Cloudanwendungen verändern den Security-Fokus

www.it-daily.net

Intel Inside®. Neue Möglichkeiten Outside.
Mehrfach ausgezeichnete Serversysteme

Schichtwechsel!

Multidimensional mit neuen Intel®-Prozessoren

intel XEON® PLATINUM inside™

interemotion.com

Besuchen Sie uns auf
der CEBIT 2018
Halle 13, Stand 14/15

Wechseln Sie jetzt zur neuesten Generation TAROX Server mit Intel® Xeon® Platin-Prozessor

- Maximale Performance für Ihre Applikation mit hoch skalierbarer Architektur
- Flexible interne Datenspeicherkonfigurationen
- Integrierte Sicherheitsfunktionen zum Schutz der Hardware
- Neuste Generation der Netzwerkkomponenten für einen effizienteren Datentransfer
- Optimiertes Energie- und Temperaturmanagement
- Verbessertes Ressourcenmanagement

Diesen Artikel finden Sie unter **www.tarox.de**

25 IT. JUBILÄUM. TAROX. 1993 – 2018.

www.tarox.de

TAROX Aktiengesellschaft | Stellenbachstr. 49 – 51 | 44536 Lünen | Telefon: +49 (0)231 / 98 98 0-300 | vertrieb@tarox.de

4
COVERSTORY

10

INHALT

IT-SICHERHEIT

DIGITALISIERUNG, IOT, CYBERSECURITY & SOME MORE.

Der TÜV TRUST IT hat eine weitere Zunahme der Vielfalt und Intensität von Sicherheitsbedrohungen prognostiziert. Dazu hat Geschäftsführer Detlev Henze neun Thesen formuliert.

1 Skriptbasierte Schadsoftware verschärft die Bedrohungslage

Schadsoftware setzt zunehmend auf skriptbasierte Sprachen wie Visual Basic Script (VBS), JavaScript oder PowerShell. Der Grund dafür ist, dass die Zielsysteme die Interpreter für diese Sprachen häufig direkt zur Verfügung stellen, sodass die Schadsoftware ohne Umwege ausgeführt werden kann. Hinzu kommt ihre schwierige Identifikation als Schadsoftware, da diese Sprachen auch von Administratoren eingesetzt werden und es demnach schwer zu unterscheiden ist, ob es sich um legitime oder schädliche Aktivitäten handelt. Zudem bewegt sich skriptbasierte Schadsoftware „unter dem Radar", weil sie kaum Spuren auf der Festplatte hinterlässt und somit durch klassische AV-Software nur schwer erkennbar ist.

2 Kommerzialisierung von Cyber Security-Angriffen

Durch Bitcoins und Ransomware wurde ein ebenso einfaches wie effektives Geschäftsmodell für Hacker gefunden. Es wird zunehmend genutzt, auch 2018 wird es erneut einen neuen Spitzenwert bei der Zahl dieser Cyber-Attacken geben. Parallel dazu wird der Schaden steigen, weil in den Unternehmen die Bedrohungslage und Bewertung der eigenen Sicherheitssituation unverändert deutlich auseinanderklaffen.

3 Wachsende Zwänge zu Security by Design

Wer bei der Konzeption und Architektur von Software-Lösungen und Apps nicht bereits im frühen Planungsstadium Sicherheitsaspekte mit berücksichtigt, wird es später schwer haben, ihre Sicherheit zu gewährleisten. Zumal sich auch hohe wirtschaftliche Risiken darin verbergen, denn wenn etwa bei IoT-Produkten Sicherheitsdefizite erst nach der Vermarktung durch die Nutzer festgestellt werden und die Software mit der Hardware fest verbaut wird, sind nachträgliche Korrekturen kaum noch möglich. Deshalb wird sich zunehmend ein Mentalitätswandel durchsetzen, in der Softwareentwicklung definierte Schutzziele einzubeziehen und sich an anwendungsbezogenen Bedrohungsmodellen zu orientieren. Dabei müssen konkrete Sicherheitsanforderungen explizit im Anforderungsprozess erhoben werden. Auch die Testmethoden werden sich dabei ändern, ebenso wie eine Auswahl von Testtools unter Sicherheitsaspekten erfolgen wird. Wichtig ist zu diesem Zweck aber zudem, dass entsprechende Fortbildungsprogramme für die Entwickler aufgesetzt werden.

> DIE BEDROHUNGSSZENARIEN IN DEN UNTERNEHMEN SIND VIELFÄLTIG, KOMPLEX UND OHNE HILFE VON AUSSEN KAUM ZU BEWÄLTIGEN.
>
> Detlev Henze, Geschäftsführer TÜV Trust IT https://it-tuv.com/

4 Entwicklung von IoT-Produkten benötigt KI-Methoden

Je umfangreicher das Angebot an vernetzten Consumerprodukten wird, desto vielfältiger wird das Gefahrenpotenzial. Dies hat das aus einem Verbund von gekaperten IoT-Geräten entstandene Botnetzwerk „Mirai" deutlich gemacht. Mit Spitzen-Bandbreiten von über einem Terabit/Sekunde wurden selbst Anbieter in die Knie gezwungen, die eigentlich noch am besten gegen DDoS-Angriffe gewappnet sind. Doch nicht nur DDoS-Angriffe, auch weitere Szenarien sind mit IoT-Botnetzen möglich. Was passiert beispielsweise, wenn zahlreiche von Angreifern kontrollierte Kühlschränke, Kaffeemaschinen, Wasserkocher etc. gleichzeitig ihren Energieverbrauch maximieren: Kann dann noch die Stromversorgung aufrechterhalten werden? Problematisch ist jedoch, wie selbst bei einem konsequenten Security by Design über eine Berücksichtigung der bekannten Bedrohungen hinaus auch mögliche zukünftige und noch unbekannte Zugriffsrisiken berücksichtigt werden können. Hierfür bedarf es Methoden der Künstlichen Intelligenz, mit deren Hilfe sich neue Bedrohungsmuster antizipieren lassen. Sie in der Entwicklung von IoT-Produkten zu berücksichtigen, steigert nicht nur die Sicherheitsperformance, sondern mindert auch das wirtschaftliche Risiko, da durch erst spät erkannte Security-Schwächen

Produkte möglicherweise aufwändig modifiziert oder wieder vom Markt genommen werden müssen.

5 Tool-Zoo lässt neue Risiken entstehen

Unternehmen setzen für die immer komplexeren Sicherheitsgefahren reflexartig immer mehr Werkzeuge für spezifische Anforderungen ein und bauen sich damit einen unübersichtlichen Tool-Zoo auf. Meist findet jedoch keine Prüfung statt, wie die verschiedenen Werkzeuge miteinander harmonieren. Damit entsteht die Gefahr, dass die Tools selbst zu einer Bedrohung werden.

6 Die Umsetzung der EU-DSGVO kommt unverändert nur langsam voran

Auch wenn es verbindliche zeitliche Pflichten gibt, zeigen alle derzeitigen Studien, dass sich die Unternehmen erst zurückhaltend der neuen europäischen Datenschutzverordnung widmen. Diese Zurückhaltung wird vermutlich erst aufgegeben, wenn sich den Firmen ein zusätzlicher Investitionsanreiz bietet. Er könnte darin bestehen, dass sich der notwendige Aufbau eines Datenschutzmanagementsystems (DSMS) an der Vorgehensweise eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001:2013 orientiert. Denn dies wird dazu führen, dass gleichzeitig wesentliche Voraussetzungen für den Aufbau eines zertifizierbaren ISMS geschaffen werden, was einen höheren Investitionsnutzen mit sich bringt.

7 IT-Sicherheitsgesetz erzeugt Domino-Effekte in Richtung der Lieferanten

Das IT-SiG bleibt unverändert weit oben auf der Agenda, da es sich kontinuierlich weiterentwickelt. Vor allem aber müssen im Mai 2018 die betroffenen Unternehmen aus dem sogenannten Korb 1 mit den Sektoren Energie, Informationstechnik, Telekommunikation, Wasser und Ernährung die Umsetzung der Sicherheitsmaßnahmen gemäß § 8a nachweisen. Spannend wird es hier bei der Frage, wie die öffentlichen Institutionen dann mit den „schwarzen Schafen" unter den nachweispflichtigen Firmen umgehen werden.

Unabhängig davon werden die KRITIS-Unternehmen die von ihnen zu erfüllenden Sicherheitserfordernisse zunehmend auch an ihre Lieferanten übertragen, weil in einer digitalisierten Welt die Sicherheitsverhältnisse nicht an den Grundstücksmauern des eigenen Unternehmens Halt machen. Die KRITIS-Firmen werden deshalb insbesondere Anforderungen in Richtung eines zertifizierbaren Informationssicherheitsmanagementsystems nach ISO 27001 an ihre Lieferanten stellen.

8 Sicherheitsniveau des autonomen Fahrens noch unzureichend

Abgesehen davon, dass Fahrerassistenzsysteme noch nicht unbedingt nach Security by Design-Anforderungen entwickelt werden und noch eine Reihe Kinderkrankheiten aufweisen, bestehen noch zahlreiche offene Fragen. So fehlt es noch an ausreichenden Verfahren für die Validierung von Funktionen für das Hochautomatisierte Fahren (HAF) sowie an Methoden für den Software-Download bzw. Überprüfung der fortschreitenden Automatisierungsfunktionen in den Fahrzeugen. Erkenntnisse relevanter Forschungsprojekte und von Testumgebungen für HAF sollten in Genehmigungsprozessen, Zertifizierungs- und Zulassungsverfahren einfließen, damit diese ökonomisch umsetzbar werden. Ebenso bedarf es einer verstärkten Fokussierung auf Fail-safe Ansätze von HAF-Systemen.

Zudem sind die Herausforderungen an die Übertragung sicherheitsrelevanter Daten von Fahrzeugen an eine übergeordnete Plattform und die Bereitstellung sicherheitsrelevanter Informationen an alle vernetzten Teilnehmer in gleicher Aktualität und Qualität noch nicht angemessen gelöst. Und nicht zuletzt: Es gilt, den Sicherheits- und Datenschutzerfordernissen durch adäquate Verschlüsselungstechnologien und qualifizierte Auditierungen Rechnung zu tragen.

9 Produktion

Mit Blick auf die Industrie 4.0-Zukunft hat auch die Digitalisierung der Produktionsstrukturen eine deutlich höhere Dynamik bekommen, allerdings entspricht die wachsende Vernetzung noch längst nicht den notwendigen Sicherheitsanforderungen. Dadurch können die IP-basierten Fertigungssysteme bis hin zu den Leitständen ein Einfalltor in das gesamte Unternehmensnetz werden. Zu welchen Konsequenzen mit längeren Produktionsstillständen dies führen kann, mussten in diesem Jahr bereits marktbekannte Unternehmen erfahren. Daraus leitet sich die Empfehlung ab, mit dem Sicherheitsengagement in der Fertigung nicht erst bis zur Umsetzung umfassender Industrie 4.0-Infrastrukturen zu warten.

CEBIT 2018

SECURITY WIRD ZU EINEM TOPTHEMA.

11.-15. JUNI IN HANNOVER

Die Meldungen über Hacker-Angriffe oder Cybercrime-Attacken gehören schon fast so selbstverständlich zur täglichen Nachrichtenlage wie der Wetterbericht. Ob Politik, Wirtschaft, Verwaltung oder Gesellschaft – im Jahr 2018 kommt niemand an IT-Sicherheit und Data Security vorbei. Deshalb flaggt die neue CEBIT im Juni 2018 Security auch als eines ihrer Topthemen aus.

Und das aus gutem Grund: In einer aktuellen Umfrage des Bitkom sieht Deutschlands Wirtschaft großen Nachholbedarf beim Thema IT-Sicherheit. Demnach wollen drei von vier Unternehmen ihre Investitionen in IT-Sicherheitslösungen im Jahr 2018 steigern.

Die CEBIT informiert im Juni sowohl im Ausstellungsbereich als auch in Form von Vorträgen und Diskussionen auf verschiedenen d!talk-Bühnen über alle Themen rund um IT-Sicherheit und Data Security. Sicherheitsverantwortliche und IT-Professionals von großen und mittleren Unternehmen sowie Firmenlenker und Anwender von kleinen Betrieben und Startups können sich unter anderem darüber informieren, mit welchen Tools und Strategien Cyberangriffe erkannt werden und wie sie beim Aufbau der IT-Sicherheit unterstützt werden. Experten präsentieren erste Best-Practice-Szenarien zur Umsetzung der EU-Datenschutzverordnung und berichten über ihre Erfahrungen bei der Implementierung. Spezielle Vortragsveranstaltungen zu effizienten und kostenbewussten IT-Sicherheitslösungen wenden sich explizit an kleine Unternehmen und den Mittelstand.

Informieren und lernen

Bei der Center Stage in Halle 12 geht es unter anderem um neue und zukünftige Gefahren im Netz. Hier wird zum Beispiel die Europäische Cybersecurity-Strategie diskutiert und die Bedeutung von IT-Sicherheit in der Zukunft erläutert. Besonders interessant dürfte das Cyber Security Summit am Dienstag, 12. Juni sein. Die Opening Keynote hält der weltweit gefragte Security-Experte Mikko Hypponen, Chief Research Officer des finnischen Sicherheitsanbieters F-Secure. Er berichtet über mögliche Angriffsszenarien und wie man sich vor Cyber-Attacken schützen kann.

Über die aktuellen Trends im Bereich Cyber Security sprechen auch der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Arne Schönbohm sowie Prof. Udo Helmbrecht, Executive Director der Agentur der Europäischen Union für Netzwerk- und Informationssicherheit (ENISA).

Bei der Expert Stage in Halle 12 stehen Security Showcases und einzelne Sicherheitstechnologien auf dem Programm. Themen sind beispielsweise IT-Sicherheit für Fintech-Unternehmen sowie Sicherheit im Umfeld von IoT (Internet der Dinge) und KI (Künstliche Intelligenz). Spannend dürften vor allem die Vorträge rund um das Thema Awareness sein, also wie sensibel Mitarbeiter mit den Daten und Geräten ihres Unternehmens umgehen.

Auch die jungen IT-Unternehmen befassen sich intensiv mit Security-Anwendungen und bringen neue Lösungen mit auf die CEBIT. Im Startup-Bereich scale11 in Halle 27 wird es eine eigene Community Area rund um das Thema Security geben mit nationalen und internationalen Anbietern, unter anderem aus Frankreich, Taiwan und der Ukraine.

www.cebit.de

CEBIT®

Die Wikinger kommen, um uns zu retten

Clavister ist ein schwedisches Cybersicherheitsunternehmen mit der festen Überzeugung, dass robuste Netzwerksicherheit jedermanns Sache ist. Mit einem virtuellen und physischen Ökosystem schützen wir Geschäftsprozesse und stellen sicher, dass unsere Kunden die bestmögliche Sicherheit vor der wachsenden Bedrohungslandschaft haben. Wir haben heute zwar Schwert und Axt gegen Code eingetauscht, aber wir haben nach wie vor unseren Wikingergeist, der besagt, dass die beste Cyber-Verteidigung ein starkes Sicherheitssystem ist.

Erfahren Sie mehr unter clavister.com/Vikings

clavister®
CONNECT. PROTECT

DSGVO BETRIFFT ALLE DATEN

ALLE EBENEN EINES UNTERNEHMENS MÜSSEN KONTINUIERLICH ZUSAMMENARBEITEN.

> ES WIRD DEUTLICH, DASS ALLE EBENEN EINES UNTERNEHMENS KONTINUIERLICH ZUSAMMENARBEITEN MÜSSEN, UM RECHTMÄSSIG IM SINNE DER DSGVO ZU HANDELN.
>
> Sven Sellen, Security Specialist, Ivanti | www.ivanti.de

In Kürze tritt die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft. Doch fast die Hälfte der deutschen Unternehmen hat laut IDC-Umfrage noch keine konkreten Maßnahmen zur Compliance getroffen. Offensichtlich rechnen sie nicht mit Kontrollen oder unterschätzen die möglichen Folgen von Verstößen. Doch Unternehmen sollten auf Nummer Sicher gehen. Was sie dabei zu beachten haben, erläutert Sven Sellen, Security Specialist bei Ivanti, im Interview.

it security: *Herr Sellen, wo liegen die größten Herausforderungen, die ein Unternehmen in punkto DSGVO zu lösen hat?*

Sven Sellen: Die zentrale Botschaft der DSGVO lautet: Für eine Umsetzung der Verordnung reicht Technologie alleine nicht aus. Es handelt sich vielmehr um eine unternehmensorganisatorische Aufgabe, die alle Bereiche einer Firma betrifft. Verkürzt dargestellt, müssen Unternehmen dazu insgesamt sieben Prinzipien parallel in Einklang bringen:

- Eine Datenverarbeitung muss rechtmäßig und transparent erfolgen.
- Daten dürfen nur für legitime Zwecke verarbeitet und gespeichert werden.
- Das Prinzip der Datenminimierung zwingt Firmen dazu, nur die notwendigsten Informationen zu verwenden.
- Dabei müssen aktuellen Systeme zum Einsatz kommen, die exakte und gültige Daten verarbeiten.
- Unnötige Redundanz und Kopien von Daten müssen vermieden werden.
- Es gilt das Prinzip der vertraulichen und sicheren Datenspeicherung.
- Und letztlich müssen Unternehmen zudem die Einhaltung der DSGVO nachweisen können.

Aus dieser Übersicht wird deutlich, dass alle Ebenen eines Unternehmens kontinuierlich zusammenarbeiten müssen, um rechtmäßig im Sinne der DSGVO zu handeln. Wenn nicht: Die Strafen für Verstöße liegen bei 10 bis 20 Millionen Euro oder 2 bis 4 Prozent des weltweiten Umsatzes, je nachdem welcher Betrag höher ist. Unklar ist jedoch derzeit noch, wie rigide die EU Verstöße ahnden wird.

it security: *Wo liegen die größten Hindernisse für die Umsetzung dieser Prinzipien?*

Sven Sellen: Oft fehlt ein Anstoß durch den CIO oder CEO, der letztlich für die Compliance verantwortlich ist. Er muss für einen Ruck sorgen, der durch das ganze Unternehmen geht. Denn heute arbeiten IT-Betrieb und IT-Security sowie Fachabteilungen getrennt voneinander in Silos. Doch die

DSGVO betrifft technische Sicherheitsmaßnahmen, organisatorische Prozesse und den Umgang der Mitarbeiter mit personenbezogenen Daten gleichermaßen. Streng genommen müssen Firmen alle Unternehmensdaten im Auge behalten – denn aus nahezu jeder Information lässt sich ein Personenbezug herstellen.

Meiner Ansicht nach liegt der Schlüssel zur DSGVO bei den Mitarbeitern. Zum Beispiel speichern Vertriebler Kunden-Angebote auf ihrem Tablet. Bleibt das Gerät unbeaufsichtigt im Auto oder dem Büro eines Kunden liegen, ist die DSGVO schon verletzt. So sind mobile Arbeitsgeräte immer mitzunehmen oder in einem Safe einzusperren. Solche und ähnliche Anforderungen führen zu Mehraufwand und werden gerne daher einmal ignoriert. Hier muss die IT-Abteilung steuernd eingreifen und beispielsweise Security-Funktionalitäten bereits im IT-Betrieb verankern und Prozesse soweit wie möglich automatisieren. Wir nennen das Operational Security.

it security: *Wie lassen sich Endgeräte technisch schützen?*

Sven Sellen: Dazu gehören in erster Linie System Patching, 3rd Party Patches, Applikationskontrolle, Rechteverwaltung, Device Control, Antivirus, Verschlüsselung und Discovery. Gerade Drittanbieter-Software ist heute das Haupteinfallstor für Cyberkriminelle und nicht mehr die klassische „Windows-Lücke". Mit diesen sieben Maßnahmen lassen sich unserer Erfahrung nach etwa 95 Prozent aller IT-Risiken am Endgerät eindämmen. Eine hundertprozentige Sicherheit gibt es allerdings nicht. Man kann es Hackern nur schwer machen.

Zugleich muss sich die IT-Abteilung gegen einen möglichen Datenmissbrauch durch die eigenen Mitarbeiter wappnen. Strenges Rechtemanagement wird mit der DSGVO Pflicht. Zum Beispiel sollte nicht jeder Mitarbeiter jedes Dokument auf jeden USB-Stick übertragen dürfen. Die Rechtekontrolle ist mit Hilfe von Tools auch zu automatisieren. Wenn etwa ein Mitarbeiter kündigt, sollten ihm sofort Nutzungsrechte entzogen werden, um einen vermeidbaren Informations-Abfluss zu unterbinden. Dabei unterstützen automatisierte Services für Onboarding und Offboarding, die von der HR-Abteilung mitgestaltet und gestartet werden.

it security: Dann ist die HR-Abteilung von Anfang an bei der IT-Security einzubinden?

Sven Sellen: Ja, nur dann wird ein sauberer Umgang der Mitarbeiter mit den IT-Systemen gewährleistet. Zur Unterstützung sind gemeinsam von HR und IT konzipierte Awareness-Schulungen durchzuführen. Zudem sollten sie die Prozesse anhand der Frage gestalten, wo personenbezogene Daten ausgelesen werden können. Hier werden oft viele Speicherorte übersehen, sofern es kein durchgehendes Single Sign-On gibt.

it security: *Aber bei allen Vorsichtsmaßnahmen: Müssen Unternehmen ihren Mitarbeitern nicht auch vertrauen?*

Sven Sellen: Hier ist das richtige Maß zu finden. Vertrauen ist für die Zusammenarbeit innerhalb eines Unternehmens unabdingbar. Allerdings gilt leider auch, dass Firmendaten vor allem durch interne Faktoren bedroht sind – aus Unachtsamkeit der Mitarbeiter oder leider auch absichtlich. Unternehmen sollten daher ein gesundes Misstrauen entwickeln und zum Beispiel das Prinzip der geringsten Rechte umsetzen. Das bedeutet, dass Mitarbeiter nur auf die tatsächlich von ihnen benötigten Daten und Anwendungen zugreifen dürfen. Das zieht sich bis in die IT-Abteilung: Nicht jeder Admin sollte einen vollständigen Zugang zu allen IT-Ressourcen haben. Zum Beispiel braucht ein IT-Verantwortlicher für die Fertigungsstraße keinen Zugang zu Finanz- oder HR-Daten. Ein Personaler muss nicht auf die Clients der Mitarbeiter zugreifen können. So sollten jeweils granulare Rechte entsprechend der Aufgaben umgesetzt werden.

it security: *Im Rahmen der Digitalisierung kann sich aber eine Rechte-Zuweisung schnell verändern ...*

Sven Sellen: Absolut. Daher muss das Rechte-Management auch flexibel sein. Hinzu kommt, dass nicht nur Menschen Zugriffsrechte benötigen, sondern auch Geräte. Der Netzwerk-Perimeter löst sich zunehmend auf, so dass mobile Devices wie Smartphones oder auch in der Firma installierte IP-Kameras zu berücksichtigen sind. Unternehmen brauchen daher ein umfassendes Zugriffs- und Rechtemanagement für Personen und Geräte. Genauso wichtig ist dann ein übergreifendes Patch-Management zur Absicherung von Soft- und Hardware. Selbst seit langem verfügbare Patches werden häufig nicht aufgespielt – WannaCry lässt grüßen. Diese beiden Maßnahmen sind gute Startpunkte für die Umsetzung der DSGVO.

it security: *Welche Vorgehensweise empfehlen Sie Unternehmen, die sich auf die DSGVO vorbereiten wollen?*

Sven Sellen: Die IT- und IT-Sicherheitsteams sollten sich Schritt für Schritt der DSGVO annähern. Im ersten Schritt empfehlen wir eine Bestandsaufnahme:

- Hardware-Inventarisierung: Welche firmeneigenen und privaten Geräte sind im Einsatz?
- Software-Inventarisierung: Welche Applikationen werden „an der IT vorbei" genutzt?
- Patch Management: Werden nur aktuelle Versionen eingesetzt?
- Automatisierung: Ist die Inventurliste und sind Patches auf dem neuesten Stand?
- Applikationskontrolle: Welche Anwendungen dürfen verwendet werden?
- Rechteverwaltung mit Zugriffsmanagement: Wer darf mit welchem Gerät was nutzen?
- Gerätekontrolle: Auf welche Anwendungen und Systeme darf ein Gerät von wo aus zugreifen?
- Schulungen: Wie aufmerksam sind die Mitarbeiter?

Die Informationen aus dieser Null-Messung sollten dann primär betriebsorganisatorisch berücksichtigt werden. Die IT muss hier eng mit den Fachabteilungen zusammenarbeiten, um einen gangbaren Weg zu finden. Denn nur die Fachabteilungen wissen, welche Anwendungen für welche Arbeitsprozesse wichtig sind und wo keinesfalls Beeinträchtigungen durch unnötige oder zu strenge Sicherheitsmaßnahmen geschehen dürfen. Diese Zusammenarbeit muss letztlich von oben gesteuert werden. Denn schließlich ist der CEO oder CIO für die DSGVO-Compliance verantwortlich.

it security: *Herr Sellen, wir danken Ihnen für das Gespräch*