TÜV Rheinland Cyber Security Trends 2017

Cyber-Security-Strategien müssen angepasst werden

Der bundesweit tagelange Ausfall vieler Telefon-, Internet- und Fernseh-Anschlüsse, Störungen von Energieversorgung oder Produktion und nicht zuletzt die mutmaßlichen Hacker-Angriffe auf die US-Wahl: Das Jahr 2016 war ein neuer Höhepunkt in Häufigkeit, Ausmaß und Qualität der Cyber-Attacken. Eine Entwarnung ist nicht in Sicht.

Was sind derzeit die Top-Themen der Cyber Security, und wie können sich Unternehmen und die Öffentliche Hand für die Herausforderungen von heute und morgen wappnen? Die führenden Security Analysts von TÜV Rheinland geben Auskunft.

Björn Haan, TÜV Rheinland

„Die Fülle und Verfügbarkeit von sensiblen Informationen über Menschen und Systeme werden zwangsläufig den Anpassungsdruck für gegenwärtige Cyber-Security-Strategien erhöhen."

Frank Luzsicza, TÜV Rheinland

„Cyber Security muss Teil des Business Cases sein und darf nicht als reiner Kostentreiber gesehen werden."

In den vergangenen Jahren haben Unternehmen eine erhöhte Sensibilität für die Bedrohungslage entwickelt und Cyber-Security-Budgets kontinuierlich erhöht. Angesichts der Dynamik und Komplexität der technischen Entwicklung im Kontext der digitalen Transformation ist in vielen Organisationen aber nach wie vor Luft nach oben, um die Cyber Security auch für die Anforderungen von morgen zu optimieren.

Klar ist: Wir gehen einem Zeitalter signifikanter Datenverletzungen entgegen. Konsequenz: Dem Top-Management kommt nach Auffassung von TÜV Rheinland mehr denn je eine Schlüsselrolle zu. »Die daraus resultierende Fülle und Verfügbarkeit von sensiblen Informationen über Menschen und Systeme werden zwangsläufig den Anpassungsdruck für gegenwärtige Cyber-Security-Strategien erhöhen«, ist Björn Haan, Geschäftsfeldleiter Cyber Security Deutschland ICT & Business Solutions bei TÜV Rheinland, überzeugt. Was das genau bedeutet, beleuchten die Cyber Security Trends 2017 von TÜV Rheinland. Sie spiegeln die Einschätzung der aktuellen Entwicklung seiner führenden Experten für Cyber Security in Deutschland, den USA, Europa und IMEA wider. Es folgt ein Auszug – die kompletten Cyber-Security-Trends gibt es als Whitepaper zum Download: www.tuv.com/cybersecurity-trends2017.

1. Die Wucht der Attacken steigert sich. Wer trägt die Verantwortung?

Weitere Angriffswellen werden folgen; neu ist die Wucht, mit der die Attacken geführt werden. Das wirft die zentrale Frage auf, wie sicher die vernetzten Geräte, die IT-Netzwerke und die Infrastrukturen sind. Wer trägt die Verantwortung, wenn Cyber-Security-Maßnahmen nicht ausreichen? Müssen Auflagen und Kontrollen weiter verschärft werden?

2. Das Internet der Dinge erfordert verbindliche Sicherheitsstandards

Smarte Geräte werden immer beliebter, umso dringender wird der Schutz der Privatsphäre. Eher früher als später werden Hersteller vernetzter Geräte höhere Sicherheitsstandards einführen müssen. Freiwillige oder verpflichtende Cyber-Security-Prüfungen und Zertifizierungen für vernetzte IoT-Geräte vor der Markteinführung werden wahrscheinlicher.

3. 2017 wird das Jahr der Cloud-Security-Lösungen

Die Sensibilität dafür, dass beim Einsatz von Cloud Services das IT-Netzwerk noch besser abgesichert werden muss, steigt. Sicherheitslösungen, die den Netzwerkverkehr zwischen dem Cloud-nutzenden Unternehmen und dem Cloud Service Provider überwachen, werden verstärkt nachgefragt. Außerdem ist die Cloud selbst immer häufiger Quelle für den Abruf von Sicherheitslösungen, darunter Echtzeit-Sicherheitsanalysen und die Detektion von Anomalien durch Künstliche Intelligenz (maschinelles Lernen), aber auch Managed Services für Security Data Analytics, Continuous Monitoring und Incident Response Advisory Services.

Bild: Fotolia / sudok1

4. Das neue Traumpaar: IAM und die Cloud

IAM (Identity-and-Access-Management) und Cloud werden zur neuen äußeren Verteidigungslinie der Organisation. Cloud-Strategien werden stärker mit dem Bereich Rechte-, Zugriffs- und Password-Management verzahnt. Das Ergebnis sind eine konsistente Verwaltung von Benutzern und Berechtigungen über Rollen sowie eine sichere und benutzerfreundliche Authentisierung.

5. Bevorzugte Angriffsziele: Patientenakten und Medizingeräte

Das Gesundheitswesen steht 2017 noch stärker im Fadenkreuz der Hacker. Medizinische Einrichtungen werden überzeugende Antworten dafür finden müssen, wie sie vernetzte medizinische Geräte in ihrem Netzwerk und sensible Patientendaten künftig besser schützen wollen. Hersteller von Medizingeräten ziehen immer öfter unabhängige Dritte zu Sicherheitsaudits heran, um den verschärften Datenschutzanforderungen in Europa genügen zu können.

6. Managed Security Services: Es geht nicht mehr ohne

Viele Unternehmen stehen der Auslagerung von Cyber Security an externe Partner nach wie vor kritisch gegenüber. Angesichts des anhaltenden Fachkräftemangels wird Vertrauen zu einem kompetenten externen Partner für Cyber Security zu einem der wichtigsten Erfolgsfaktoren für die Absicherung des Unternehmens, nicht zuletzt auch wegen der wachsenden Zahl von Innentätern.

7. Industrie 4.0: Funktionale Sicherheit und Cyber Security gehen stärker Hand in Hand

Industrie und Kritische Infrastrukturen sind mehr denn je der Gefahr unberechtigter Zugriffe ausgesetzt. Weil die IT wesentlich ist für die funktionale Sicherheit in der Fertigung, für den sicheren Datenaustausch und für die Verfügbarkeit und Ausfallsicherheit vernetzter Systeme, müssen funktionale Sicherheit und Cyber Security noch stärker Hand in Hand arbeiten. Gerade Unternehmen der vernetzten Industrie (Industrie 4.0) müssen die Sicherheit ihrer Produkte über den gesamten Lebenszyklus hinweg im Blick haben und die Risiken permanent überwachen.

8. Schlüsselfaktor Endgeräte-Sicherheit

Endgeräte wie Laptops, mobile Geräte, Desktop-Rechner, Server und vernetzte Geräte zählen zu den am einfachsten zu kapernden Einfallstoren für Angreifer. Die Experten von TÜV Rheinland empfehlen dringend, mindestens die Standardmaßnahmen auszuschöpfen, die den Schutz vor Angriffen steigern.

9. Das Ende des Silo-Denkens? eGRC und IT-GRC wachsen zusammen

Die integrierte Sicht von IT- und Business-Risiken verbessert nicht nur das Reporting gegenüber Aufsichtsbehörden, sondern erlaubt auch einen unverstellten Blick auf die tatsächliche Risikoexposition und zu schützende Werte der Organisation. Das ermöglicht der Unternehmensführung eine deutlich höhere Entscheidungsqualität. Angesichts verschärfter gesetzlicher Anforderungen wie der EU-Datenschutzgrundverordnung und mit Blick auf den Schutz des geistigen Eigentums ist das für Unternehmen von vitaler Bedeutung.

Angesichts dieser Herausforderungen ist auch klar: Dem Top-Management kommt mehr denn je eine Schlüsselrolle zu. Awareness für Cyber Security als Wettbewerbsvorteil und erfolgskritischer Faktor ist nicht nur eine Frage des fachlichen Verständnisses, sondern auch eine Aufgabe der Kommunikation zwischen CISO, CIO und CEO. Wichtig ist, dass Spezialisten für Cyber Security ihre Inhalte Management-gerecht und verständlich formulieren. Frank Luzsicza, Leiter des Geschäftsbereichs ICT & Business Solutions bei TÜV Rheinland, fordert einen generellen Paradigmenwechsel bei Unternehmen und der Öffentlichen Hand: »Cyber Security muss Teil des Business Cases sein und darf nicht als reiner Kostentreiber gesehen werden. Cyber Security ist idealerweise sowohl Risiko-Beratung als auch Business Enabler.«

In den USA haben Organisationen schon vor längerem begonnen, ihre Risiko-Management-Programme mit Fokus auf ihr Business umzugestalten, und zwar auf Basis gut durchdachter GRC-Strategien und Assessment-Methoden wie FAIR (Factor Analysis of Information Risk). Dabei werden die Faktoren ermittelt, die zu Risiken für die Organisationen werden können, und analysiert, wie sie sich gegenseitig beeinflussen. Damit die interne Kommunikation zwischen den Entscheidern besser funktioniert, hat die National Association of Corporate Directors in den USA einen Handlungsleitfaden entwickelt, der das Miteinander des Top-Managements mit CIO und CISO regeln soll. Das Orientierungspapier ist gut durchdacht. Es fokussiert typische Sichtweisen aller Beteiligten auf die Top-Risiken und geht der Frage nach, wie damit im Einzelfall umzugehen ist. Ein beispielhafter Ansatz, von dem alle profitieren können, denn eine proaktive Cyber-Security-Strategie wird in Zukunft vitaler Erfolgsfaktor für alle sein – besonders mit Blick auf die Dynamik von Digitaler Transformation, Industrie 4.0 und vernetzten, intelligenten Geräten im IoT. (ak) ■

Strategien rund um die sichere digitale Transformation

IT-Sicherheits-Kongress von TÜV Rheinland

Unternehmen können ihre Kompetenz und ihr Know-how rund um Cyber Security und Strategien für eine sichere digitale Transformation demnächst vertiefen, und zwar auf dem IT-Sicherheits-Kongress 2017 von TÜV Rheinland.

Unter dem Titel „Cyber Security und Qualität in der digitalen Transformation" erläutern am 7. und 8. November 2017 in Frankfurt am Main nationale und internationale Experten traditionelle Themen der Informations- und IT-Sicherheit sowie sicherheitsrelevante Aspekte der digitalen Transformation von heute und morgen. Informieren kann man sich darüber hinaus über branchenübergreifende Best-Practice-Erfahrungen aus den Bereichen Smart Devices, Digital Factory, Cyber Security und Future Workplace. Konkrete Lösungen zu Sicherheitsaspekten in der Digitalisierung runden das Programm ab. (ak)