TÜV Rheinland: Was bringen die Cyber Security Trends 2017?

Mehr erfahren über die sichere digitale Transformation auf dem IT-Sicherheits-Kongress 2017.

Stefanie Ott

Vorspann

Mit welchen Cyber-Herausforderungen haben Unternehmen und die Öffentliche Hand in den nächsten Monaten zu rechnen? Das beleuchten die Cyber Security Trends 2017 von TÜV Rheinland. Führende Experten für Cyber Security identifizieren aktuelle Herausforderungen und Lösungsansätze für Wirtschaft und öffentliche Einrichtungen. Mehr unter

↗ www.tuv.com/cybersecuritytrends2017

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

Weitere Angriffswellen werden folgen, neu ist die Wucht der Attacken. 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. Freiwillige oder verpflichtende Cyber Security-Prüfungen und Zertifizierungen für vernetzte IoT-Geräte (IoT = Internet of Things, Internet der Dinge) 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 rund um Cloud Services werden verstärkt nachgefragt. Außerdem ist die Cloud selbst immer häufiger Quelle für den Abruf von Sicherheitslösungen.

4. Das neue Traumpaar: IAM und die Cloud.

Rollen- und Zugriffsmanagement (IAM = Identity-und-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 ist eine sichere und benutzerfreundliche Authentisierung.

5. Bevorzugte Angriffsziele: Patientenakten und Medizingeräte.

Das Gesundheitswesen wird vernetzte medizinische Geräte sowie sensible Patientendaten 2017 künftig noch besser vor Hackern schützen müssen, auch, um den immer schärferen Auflagen der Aufsichtsbehörden genügen zu können.

6. Managed Security Services: Es geht nicht mehr ohne.

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 an Innentätern.

Zweitägiger Kongress rund um alle sicherheitsrelevanten Aspekte der digitalen Transformation

↗ www.tuv.com/it-sicherheits-kongress

Ihr Wissen, wie sich die Potenziale der Digitalisierung sicher nutzen lassen, können Organisationen auf dem IT-Sicherheits-Kongress 2017 von TÜV Rheinland erweitern. Unter dem Titel »Cyber Security und Qualität in der digitalen Transformation« erläutern am 07. und 08. November 2017 im Kap Europa in Frankfurt a.M. nationale und internationale Experten traditionelle Themen der Informations- und IT-Sicherheit als auch 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.

© RapidEye | iStock

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. Funktionale Sicherheit und Cyber Security müssen noch stärker Hand in Hand arbeiten. Die vernetzte Industrie (Industrie 4.0) muss 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 mindestens die Standardmaßnahmen auszuschöpfen, um den Schutz vor Angriffen zu steigern.


© sudok1 | Fotolia.de

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

Die integrierte Sicht von IT- und Business-Risiken verbessert das Reporting gegenüber Aufsichtsbehörden und erlaubt einen unverstellten Blick auf die tatsächlichen Risiken und zu schützende Werte der Organisation. Das ermöglicht der Unternehmensführung eine deutlich höhere Entscheidungsqualität. ▬

Weitere Informationen:

↗ www.tuv.com/informationssicherheit
↗ www.tuv.com/apt
↗ www.tuv.com/mss
↗ www.tuv.com/grc
↗ www.tuv.com/iam

GRC – Governance, Risk & Compliance – Unternehmen professionell managen

↗ http://tuv.li/-c

Der APT Defense Service von TÜV Rheinland:

↗ http://tuv.li/-k

Was ist ein ISMS?

↗ http://tuv.li/-m

Whitepaper Cyber Security Trends 2017
↗ www.tuv.com/cybersecuritytrends2017

TÜVRheinland®
Genau. Richtig.

TÜV Rheinland
Am Grauen Stein | 51105 Köln
Tel. +49 221 806-0
stefanie.ott@de.tuv.com | www.tuv.com