Hintergrundinformation

**TÜV Rheinland: Cybersecurity Trends 2018 im Überblick**

*Bereits zum fünften Mal seit 2014 hat ein internationales Expertenteam von TÜV Rheinland über mehrere Monate die wichtigsten Trends zur Cybersecurity weltweit analysiert und zusammengefasst. Die zentralen Fragen sind: Welche Konsequenzen haben Angriffe auf die Cybersecurity für Wirtschaft, Gesellschaft und die Menschen? Und: Wie können sich Unternehmen und Organisationen besser vor der wachsenden Zahl von Cyber-Angriffen schützen?*

Ein wichtiges Ziel der Experten von TÜV Rheinland ist es, mit den Cybersecurity Trends die Sensibilisierung für Risiken der Digitalisierung weiter zu schärfen. Das ermöglicht es wiederum, die Vorteile der Technologien für jeden einzelnen optimal nutzen zu können. Für das Jahr 2018 haben die Fachleute acht große Trends identifiziert.

Die vollständigen Materialien und die 24-seitige Analyse der Experten mit den Cybersecurity Trends 2018, finden sich unter www.tuv.com/cybersecurity-trends-2018 zum kostenfreien Download bei TÜV Rheinland.

Trend 1: Durch die wachsende Anzahl an globalen Regulierungen im Cyber-Umfeld steigt der Preis, um die Privatsphäre zu schützen.

Datenschutz ist ein kritischer Aspekt in einer immer digitaler werdenden Welt. Der 25. Mai 2018 hat einen entscheidenden Wendepunkt für den Datenschutz in Europa dargestellt. Dieses Datum markiert das Ende des Übergangszeitraums für die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, da diese seit diesem Tag rechtsverbindlich gilt. Sie bedeutet einen grundlegenden Wandel bei der Daten-Governance und der Art, wie Informationen von Unternehmen geschützt werden, die personenbezogene Daten von EU-Bürgern verarbeiten.

Die Verordnung ist der Beginn einer wachsenden weltweiten Regulierung im Bereich Datenschutz. Verstöße gegen diese können mit Strafen in Höhe von bis zu 4 Prozent des globalen Umsatzes belegt werden – eine enorme Summe, die nicht außer Acht gelassen werden darf. Es ist davon auszugehen, dass die EU-Kommission Verstöße gegen die DSGVO durch große globale Unternehmen konsequent verfolgen wird.

Trend 2: Das Internet der Dinge (Internet of Things, IoT) treibt das Zusammenspiel von Sicherheit, Cybersecurity und Datenschutz voran.

Im Jahr 2016 hat die Verwendung der Schadsoftware Mirai gezeigt, dass vernetzte und internetfähige IoT-Geräte ein schlagkräftiges und gefährliches Botnet bilden können. Als Botnets werden automatisierte Schadprogramme bezeichnet, die ganze Computernetze angreifen. Die immer kürzeren Zeitanforderungen bei der Produktentwicklung und die eingeschränkte technische Performance von IoT-Geräten sorgen heute dafür, dass solche Geräte kritische Schwachstellen aufweisen. Diese können einfach ausgenutzt werden.

Die Auswirkungen von Datenverletzungen gehen heute weit darüber hinaus, illegal erworbene Daten zu Geld zu machen. Sie umfassen vielmehr auch physische Bedrohungen für Gesundheit und Sicherheit, da Geräte und Systeme direkt mit offenen Netzwerken verbunden sind. Um die Sicherheit „smarter" und vernetzter Geräte ist es nicht gut bestellt. Schätzungen gehen davon aus, dass bis 2022 in privaten Wohnungen und Häusern über 500 solcher Geräte vorhanden sind. Damit wird klar, dass sich die Risiken für Sicherheit, Cybersecurity und Datenschutz erheblich erhöhen werden.

Trend 3: Operational Technology und die Industrie sind wichtige Angriffspunkte für Cyber-Attacken.

Das so genannte Industrial Internet sorgt bereits weltweit für eine Transformation der Industrie und Infrastruktur und verspricht mehr Effizienz, Produktivität und Sicherheit. Um im Wettbewerb bestehen zu können, werden Prozessleittechnikgeräte mit der Online-Welt verbunden, wodurch oftmals unbeabsichtigt Komponenten, die Schwachstellen aufweisen, Cyber-Angriffen ausgesetzt sind.

Fertigungsanlagen sind ebenfalls ein Angriffsziel, um an geistiges Eigentum, Geschäftsgeheimnisse und technische Informationen zu gelangen. Hinter Angriffen auf die öffentliche Infrastruktur stehen dagegen finanzielle Gründe, „Hacktivismus" und die Unzufriedenheit mit staatlichen Stellen. Die Angst vor einem „Worst-Case-Szenario", bei dem Angreifer einen Zusammenbruch von Systemen auslösen, die das Fundament der Gesellschaft bilden, war ein Thema beim diesjährigen Weltwirtschaftsforum in Davos. Industrielle Systeme sind besonders anfällig gegen Angriffe auf die Lieferkette. Das haben auch kriminelle Angreifer erkannt und begonnen, diese Systeme ins Visier zu nehmen.

Trend 4: Wenn Abwehrmechanismen für Cyber-Angriffe vorhanden sind, verlagert sich der Schwerpunkt auf die Erkennung von Bedrohungen und der angemessenen Reaktionen darauf.

Angriffe der letzten Zeit zeigen, dass im Kampf gegen erfahrene und beharrliche Cyber-Kriminelle herkömmliche Verhinderungsmechanismen allein nicht ausreichen. Heute dauert es im Schnitt 191 Tage, bis ein Unternehmen ein Datenleck erkennt. Je länger es dauert, eine Bedrohung zu erkennen und darauf zu reagieren, umso größer sind der finanzielle Schaden und der Reputationsverlust, den das Unternehmen durch den Vorfall erleidet. Derzeit allerdings entstehen in den Unternehmen teure Verweildauern, bis Datenlecks gestopft werden können. Dies hat verschiedene Gründe:

- den enormen Anstieg erfasster sicherheitsrelevanter Daten,
- die Einschränkungen von aktuellen Technologien,
- die ineffiziente Nutzung von vorhandenen Bedrohungsinformationen (Threat Intelligence),
- die fehlende Überwachung von IoT-Geräten und schließlich
- den Mangel an Cybersecurity-Experten.

Trend 5: Die Nutzung von Künstlicher Intelligenz (KI) für Cyber-Attacken und für deren Abwehr nimmt zu.

Auf ihrem Weg der digitalen Transformation werden Unternehmen in steigendem Maße zum Ziel für komplexe und hartnäckige Cyber-Attacken. Schadprogramme, so genannte Malware, werden immer smarter. Malware kann sich „intelligent" anpassen und traditionelle Erkennungs- und Beseitigungsroutinen umgehen. Angesichts des globalen Mangels an Cybersecurity-Spezialisten sind die Unternehmen dabei, das Cyber-Wettrüsten zu verlieren. Die Menge an Sicherheitsdaten überschreitet bei weitem die Kapazitäten für deren effiziente Nutzung. Das führt zu einer steigenden Anzahl von KI-fähigen Cybersecurity-Anwendungsfällen: Beschleunigung der Erkennung und Bekämpfung von Sicherheitsvorfällen, bessere Identifizierung und Vermittlung von Risiken gegenüber den Fachabteilungen und die Bereitstellung einer einheitlichen Sicht auf den Sicherheitsstatus innerhalb der gesamten Organisation.

Trend 6: Zertifizierungen werden wichtig, um das Vertrauen in Cybersecurity zu stärken.

Es herrscht weitgehend Einigkeit darüber, dass Cybersecurity und Datenschutz integrale Bestandteile einer digitalen und vernetzten Welt sind. Aber: Wie lässt sich das Schutzniveau eines Unternehmens objektiv einschätzen? Die Bedenken, ob und inwieweit Cybersecurity tatsächlich umgesetzt wird, nehmen zu. Dies führt dazu, dass bestehende und neue Standards, die Cybersecurity-Strategien international vergleichbar machen, immer stärker an Relevanz gewinnen. Für Verantwortliche von Informationssicherheit in Unternehmen und für Produkthersteller sind Zertifizierungen wichtig, um nachzuweisen, dass sie getan haben, was sie versprochen haben. Die Zertifizierungsverfahren für die Bestätigung der IT-Sicherheit von Produkten konzentrieren sich heute jedoch vor allem auf kritische Infrastrukturen und die öffentliche Hand. Wo aber bleiben die Hersteller von herkömmlichen Alltagsprodukten für Verbraucher? Hier müssen sich Produktzertifizierungen im Markt breit durchsetzen, um Verbrauchern mehr Sicherheit und Orientierung zu geben.

Trend 7: Passwörter werden durch biometrische Authentifizierungen (z.B. Fingerabdruck) abgelöst.

Das digitale Leben wird durch ein komplexes Netz aus Online-Apps bestimmt, die digitale Identität durch Benutzernamen und Passwörter geschützt. Um den Schutz hinter diesen Apps zu steigern, wird empfohlen, schwer zu erratende und komplexe Kennwörter zu verwenden und diese regelmäßig zu ändern. In der Praxis geschieht das aber nur selten. Mit der exponentiellen Zunahme der Rechenleistung und dem einfachen Zugang über die Cloud können Kennwörter in einer immer kürzeren Zeit geknackt werden. Was im Jahr 2000 noch fast vier Jahre gedauert hat, ist heute bereits in zwei Monaten erledigt. Da Kennwörter häufig gestohlen, gehackt und gehandelt werden, setzen sich beispielsweise bei Mobiltelefonen, Tablets, Laptops sowie Online-Services, Systeme mit biometrischer Authentifizierung vermehrt durch. Dazu zählen Gesichtserkennung, Fingerabdruck, Iris- oder Spracherkennung.

Trend 8: Ausgewählte Branchen stehen im Visier der Angreifer: Gesundheitswesen, Finanzdienstleistungen und Energieversorgung.

Der Großteil der Cyber-Angriffe wird von Kriminellen aus finanziellen Motiven begangen. Der Wert von Daten im so genannten Darknet hängt ab von der

Nachfrage, der Verfügbarkeit, der Vollständigkeit und ihren Nutzungsmöglichkeiten. Daher sind persönliche Informationen aus dem Gesundheits- und Finanzsektor besonders gefragt. Krankenakten kosten, je nachdem, wie vollständig sie sind, zwischen 1 bis 1.000 US-Dollar. Kreditkartendaten werden für 5 bis 30 US-Dollar verkauft, wenn die benötigten Informationen für ihre Nutzung mitgeliefert werden. Andere Cyber-Angriffe haben eher politische Motive.

Im Jahr 2018 besteht ein erhöhtes Risiko für Störungen im Bereich der so genannten „Kritischen Infrastrukturen" durch Angriffe auf den Energiesektor. Beleg dafür sind die Berichte der jüngsten Zeit über die von Russland initiierten Cyber-Attacken auf das US-Stromnetz, die vermutlich bereits seit einem oder mehreren Jahren ausgeführt werden.

www.tuv.com/cybersecurity-trends-2018

*Stand: Mai 2018*