TÜV Rheinland veröffentlicht Cybersecurity Trends 2019

08.04.2019 | Köln

Wie gut Unternehmen und große Organisationen die Sicherheit von Daten und IT in der digitalen Wirtschaft gewährleisten können, entscheidet über ihren Erfolg oder Misserfolg. Das ist eine von acht wichtigen Entwicklungen, die die Experten von TÜV Rheinland für die Cybersecurity Trends 2019 identifiziert haben. „Die moderne Welt verwandelt sich rasant in eine digitale, wissensbasierte ‚Industrie 4.0'-Wirtschaft. Dieser Wandel hat die gleiche Bedeutung wie die industrielle Revolution", erklärt Björn Haan, Geschäftsführer im Geschäftsfeld Cybersecurity Deutschland bei TÜV Rheinland. „Die existenzielle Frage für viele Unternehmen ist, ob es ihnen gelingt, die Herausforderungen an die Sicherheit in der digitalen Wirtschaft zu meistern. Möglicherweise wird es schlicht auf ein einfaches Szenario hinauslaufen: Erfolg oder Misserfolg, ohne die Möglichkeit, einen Kompromiss einzugehen."

Zum sechsten Mal veröffentlicht

TÜV Rheinland veröffentlicht die Prognosen seiner weltweit führenden Cybersecurity-Experten in diesem Jahr zum

sechsten Mal. Im aktuellen Bericht schreibt TÜV Rheinland, dass Unternehmen Cyberangriffe mehr und mehr als zentrales Geschäftsrisiko erkennen und beginnen ihre Organisation darauf ausrichten. Außerdem geht es in den Cybersecurity Trends unter anderem darum, wie stark die Cyberkriminalität Technologien wie Operational Technology (OT) in der Industrie sowie das Internet der Dinge (Internet of Things, IoT) beeinflusst, warum der Fachkräftemangel zu einem immer größeren Problem werden könnte und welche Rolle Konzepte wie „Red Teaming“ (umfassende Penetrationstests) oder agile Sicherheit voraussichtlich spielen werden. Wie in den Vorjahren wurden für den Bericht Experten für Cybersecurity von TÜV Rheinland und Unternehmen in Europa, Nordamerika und Asien nach ihrer Einschätzung gefragt.

Nachfolgend die Highlights der insgesamt acht Cybersecurity Trends, die TÜV Rheinland in diesem Jahr aufzeigt:

TREND 1: Cybersecurity ist zum Thema für die Geschäftsleitungsebene geworden

Bis vor kurzem wurde mangelnde Cybersecurity nicht als ein Geschäftsrisiko, sondern als IT-Problem betrachtet. Trotz jahrelanger Warnungen haben erst die Auswirkungen des NotPetya-Cyberangriffs im Jahr 2017 diese Ansicht geändert. Mehrere große Unternehmen meldeten Verluste als Folge dieses Angriffs, darunter die Logistikunternehmen Maersk und FedEx, das Werbeunternehmen WPP und der Haushaltswarenhersteller Reckitt Benckiser. Die genannten Unternehmen haben Berichten zufolge jeweils bis zu Hunderte Millionen Euro verloren. Das macht NotPetya zum bisher teuersten Cyberangriff in der Geschichte. Zugleich sind Verletzungen des Datenschutzes weiterhin ein Grund zur Sorge. Risiken, die von einer mangelnden Cybersecurity ausgehen, haben sich damit von einem hypothetischen Problem zu einem anerkannten

Geschäftsrisiko entwickelt. Diese Erkenntnis führt nun zu langfristigen Veränderungen beim Management von Cybersecurity-Risiken und bei der Frage danach, wer für dieses Problem zuständig ist.

TREND 2: Industrielle Cybersecurity liegt Jahre hinter der allgemeinen IT-Sicherheit zurück

In einem System der Operational Technology (OT) erkennen oder verändern Computer physikalische Prozesse, indem sie Geräte wie Elektromotoren, Ventile oder Relais steuern und überwachen. Genutzt werden sie beispielsweise von Energie- und Wasserversorgern sowie der Industrie. Obwohl mangelnde Cybersecurity von OT-Systemen („industrielle Cybersecurity“) gravierende Auswirkungen haben kann, wurde sie lange Zeit vernachlässigt und war von Gleichgültigkeit und zu geringen Investitionen geprägt. Heutzutage haben sich die Risiken einer Vernachlässigung des Schutzes von OT-Systemen aufgrund neuer Technologien und geopolitischer Spannungen grundlegend verändert. Dies gilt insbesondere für Systeme zur Sicherheitsüberwachung. Wenn etwas zu einem Angriffsziel werden kann, sollten die Verantwortlichen alles Erdenkliche unternehmen, um den Erfolg eines solchen Angriffs zu verhindern.

TREND 3: Standards stellen Herausforderung für IoT-Cybersecurity dar

Weltweit erarbeiten Normenorganisationen und Branchen die Sicherheits- und Datenschutzstandards, die für die nächste Entwicklungsstufe im Internet der Dinge (Internet of Things, IoT) und der Operational Technology (OT) erforderlich sind. Bei aller guten Absicht kann es für

Hersteller verwirrend sein und zu Zeitverschwendung führen, wenn sie herausfinden möchten, welche dieser regionalen und branchenspezifischen Standards sie berücksichtigen müssen. Besonders davon betroffen sind globale Unternehmen, die bei Entwicklung ihrer Produkte nachvollziehen müssen, wie sie deren Konformität gewährleisten können. Die Existenz konkurrierender Standards könnte daher zu Zeitverschwendung führen.

TREND 4: Der Druck durch die DSGVO stellt einen Wendepunkt für den Verbraucherdatenschutz dar

Innerhalb weniger Monate nach dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) im Mai 2018, wurden die ersten Anklagen bekannt, darunter eine Geldstrafe in Höhe von 400.000 Euro, die einem Krankenhaus in Portugal von der portugiesischen Datenschutzbehörde wegen des angeblich uneingeschränkten Zugangs zu Patientenakten auferlegt wurde. Obwohl es langsam anläuft und die ersten verhängten Geldbußen eher niedrig waren, steht fest, dass die DSGVO den Datenschutz nicht nur in der EU, sondern weltweit maßgeblich beeinflussen wird. Für die meisten Branchen wird es einfach preiswerter sein, ihre Produkte und Dienstleistungen so zu entwickeln und zu gestalten, dass sie den höchsten weltweiten Standards entsprechen, anstatt sich auf geografisch begrenzten Datenschutz zu beschränken.

TREND 5: Der Fachkräftemangel im Bereich Cybersecurity wird den Arbeitsmarkt verzerren

Die Bedeutung von Cybersecurity hat zugenommen. Es gibt jedoch nicht genügend Fachpersonal, um den

Arbeitskräftebedarf in diesem Bereich zu decken. Bis zum Jahr 2020 könnten weltweit 1,5 Millionen Fachkräfte fehlen. Bis 2021 könnte sich diese Zahl Schätzungen zufolge mehr als verdoppeln. Bei einem so extremen Fachkräftemangel treten häufig Marktverzerrungen auf: Größere, finanziell besser gestellte Organisationen und Dienstleister sind in der Lage, kompetente Mitarbeiter zu rekrutieren, während kleinere Unternehmen in einigen Branchen Probleme haben könnten. Dies macht zwangsläufig nicht nur Cybersecurity teurer, sondern wirkt sich auch auf Lieferketten aus, die große und kleinere Unternehmen wirtschaftlich miteinander verbinden. Im Sinne der langfristigen Interessen der Wirtschaft ist Cybersecurity von Bedeutung für die Allgemeinheit und sollte daher für alle zugänglich sein. Wenn dieses Problem nicht gelöst wird, wird es in der Zukunft größere Herausforderungen in dem Bereich geben.

TREND 6: Die Erkennung von und die Reaktion auf Bedrohungen hängt von der Etablierung von „Sicherheitsorchestrierung, Automatisierung und Reaktion“ (SOAR) ab

Mit dem SOAR-Ansatz (Sicherheitsorchestrierung, Automatisierung und Reaktion) können die für die Erkennung von Vorfällen benötigte Zeit verringert, die Reaktion auf Bedrohungen beschleunigt und die Auswirkungen von Cyber-Angriffen minimiert werden. Den größten Mehrwert bieten hierbei automatisierte Workflows zur Eingrenzung von Bedrohungen – sie sind entscheidend beim Umgang mit sich schnell ausbreitender schädlicher Malware. Weitere Vorteile von SOAR sind die Standardisierung von Prozessen zur Untersuchung von Cyberangriffen, eine schnellere Priorisierung und entsprechende Reaktionen, die Möglichkeit einer proaktiven Suche nach Bedrohungen und die

Verbesserung der Qualität und Effizienz von Erkennungs- und Reaktionsprozessen. Um mit SOAR eine neue Welle der Automation umzusetzen, müssen Organisationen jedoch zu einer Zeit investieren und planen, in der sich etablierte Investitionen wie Security Information & Event Management (SIEM)-Lösungen gerade erst einspielen.

TREND 7: „Red Team“-Tests und agile Sicherheit gewinnen allgemein an Akzeptanz

Die Begriffe „Red Team“-Test und „ganzheitlicher Test“ haben ihren Ursprung im Bereich der Penetrationstests. „Red Teams“ simulieren, wie ein Angreifer unter realen Bedingungen durch das Ausnutzen vorhandener Schwachstellen in ein Unternehmen eindringen und sich Zugang zu Ressourcen verschaffen kann. Während Schwachstellen bei vielen Ressourcen (Anwendungen, Geräten oder Infrastrukturen) gefunden werden können, simulieren „Red Teams“ darüber hinaus Themen wie Social Engineering, Hijacking von Social Media, den physischen Zutritt zu einem Gebäude oder – in extremen Fällen – eigene Mitarbeiter mit böswilligen Absichten. Im Gegensatz zu herkömmlichem Pen-Testing versucht Red Teaming zu verstehen, wie diese Faktoren zusammenspielen und betrachtet sie nicht getrennt voneinander. Parallel dazu kommt agilen Sicherheitstests eine größere Bedeutung zu. Deren Ziel ist es, noch während der Entwicklung einer Software möglichst viele Schwachstellen zu beseitigen.

TREND 8: Cybersecurity entscheidet über Gewinner und Verlierer der digitalen Wirtschaft

Die moderne Welt entwickelt sich rasant zu einer digitalen,

wissensbasierten „Industrie 4.0“-Wirtschaft. Dieser Wandel hat eine ähnliche Bedeutung wie die industrielle Revolution im 18. Jahrhundert. Eine grundlegende Herausforderung dieses Prozesses besteht darin zu erkennen, wie die eigene Sicherheit gewährleistet werden kann, woher die Ressourcen dafür kommen sollen und welche globalen Standards erforderlich sind, um die Entwicklung so reibungslos wie möglich zu gestalten. Die Fähigkeit, die Herausforderungen an die Sicherheit in der digitalen Wirtschaft zu meistern, wird über den Erfolg von Wirtschaftssektoren, Volkswirtschaften und vielleicht sogar von politischen Systemen entscheiden, auf denen sie aufbauen. Es ist möglich, dass dies für viele große Organisationen auf ein einfaches Szenario von entweder Erfolg oder Misserfolg ohne einen Mittelweg hinauslaufen wird.

Mehr Informationen und Einschätzungen von TÜV Rheinland zu den Herausforderungen 2019 im Whitepaper Cybersecurity Trends 2019 http://www.tuv.com/cybersecurity-trends-2019.

Kontakt für Journalisten: Norman Hübner
Telefon: +49 221 806 - 3060
E-Mail: norman.huebner@de.tuv.com

****

TÜV Rheinland ist ein weltweit führender unabhängiger Prüfdienstleister mit fast 150 Jahren Tradition. Im Konzern arbeiten über 20.000 Menschen rund um den Globus. Sie erwirtschaften einen Jahresumsatz von 2 Milliarden Euro. Die unabhängigen Fachleute stehen für Qualität und Sicherheit von Mensch, Technik und Umwelt in fast allen Wirtschafts- und Lebensbereichen. TÜV Rheinland prüft technische Anlagen, Produkte und Dienstleistungen, begleitet Projekte, Prozesse und Informationssicherheit für

Unternehmen. Die Experten trainieren Menschen in zahlreichen Berufen und Branchen. Dazu verfügt TÜV Rheinland über ein globales Netz anerkannter Labore, Prüfstellen und Ausbildungszentren. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption.

Website www.tuv.com