Präsentation der Cybersecurity-Studie: Andreas Tomek (KPMG), Peter Gerdenitsch (RBI International AG), Martin Stierle (Austrian Institute of Technology), Alexander Janda (KSÖ), Vanessa Langhammer (Rail Cargo Austria AG), Peter Uher (A1 Telekom Austria).

Wissen, schützen, erkennen

Die „Cyber-Security-Studie 2019" beschäftigt sich mit der Frage, wie Unternehmen der Internetkriminalität begegnen und welche Sicherheitsmaßnahmen im Bereich Cybersecurity getroffen werden.

Cybersecurity ist die Grundlage für eine erfolgreiche Digitalisierung", sagte DI (FH) Robert Lamprecht, MSc, Director bei *KPMG Austria GmbH,* bei der Präsentation der „Cyber-Security-Studie 2019" am 8. Mai 2019 gemeinsam mit dem *Kuratorium Sicheres Österreich (KSÖ)* bei der *A1Telekom Austria AG* in Wien. „Damit Cyber-Risiken nicht zu Cyber-Vorfällen werden, ist es erforderlich, dass sich heimische Unternehmen mit Cybersecurity nachhaltig auseinandersetzen", sagte Lamprecht. Die *KPMG Austria GmbH* ist das größte Wirtschaftsprüfungs- und Beratungsunternehmen Österreichs. Es unterstützt und berät Unternehmen im richtigen Umgang mit Cyber-Risiken nach dem Motto: Wissen, schützen, erkennen und reagieren.

Die Studie beschäftigt sich mit der Frage, wie österreichische Unternehmen der Internetkriminalität begegnen und welche Sicherheitsmaßnahmen im Bereich Cybersecurity getroffen werden. Dazu wurden im Februar und März dieses Jahres Vertreter von 342 österreichischen Unternehmen befragt, darunter Klein- und Mittelbetriebe, Großunternehmen, Banken, Technologieunternehmen, Medien und Telekommunikation, öffentlicher Sektor, Industrie, Dienstleistung, Versicherung, Energiewirtschaft, Bauwirtschaft und Immobilien, Healthcare, Automotive, Retail, Food and Drink, Education und Verkehr, Transport und Logistik. Im Zuge der Präsentation, mit anschließender Podiumsdiskussion wurden folgende Fragen erörtert. Welchen neuen Bedrohungen aus dem Internet müssen wir uns 2019 stellen? Wie resilient sind unsere Systeme und Prozesse, und in weiterer Folge auch unsere Gesellschaft, im Falle eines Cyber-Angriffs? Wie gehen österreichische Unternehmen mit den neuen Herausforderungen im technologischen Alltag um?

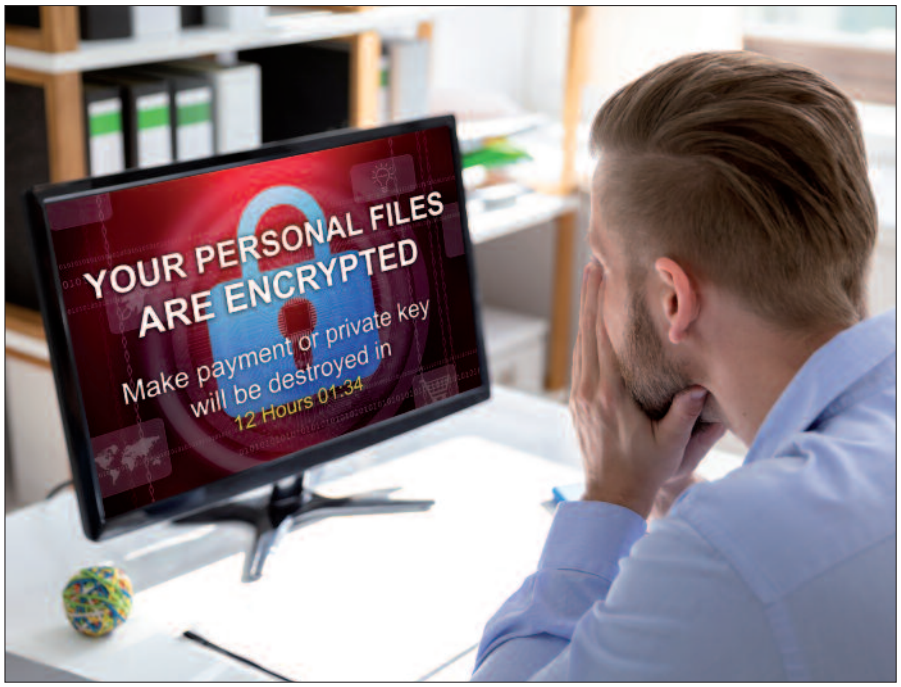
Nach Auffassung von Mag. Erwin Hameseder, Präsident des KSÖ, hat bereits ein Umdenken in den Bereichen Cybersecurity, IT-Sicherheit und digitale Sicherheit in österreichischen Unternehmen stattgefunden. Die Themen würden zwar immer öfter auf der Aufsichtsrats-, Vorstands- oder Führungsebene diskutiert, der richtige Zugang zu den Themen sei jedoch noch nicht gefunden. Es ist Aufgabe der Führungskräfte, notwendige von übertriebenen Maßnahmen zu unterscheiden und Ressourcen so einzusetzen, dass sowohl das Wachstum als auch der Schutz vor virtuellen Gefahren abgedeckt und Organisationsaufgaben weiterhin erfüllt werden können. „Genau hier setzt die Cyber-Security-Studie 2019 an. Denn das Wissen um die Bedrohungen ist genauso wichtig, wie das Lernen von den Erfahrungen anderer", erklärte Hameseder.

Robert Lamprecht: „Unternehmen müssen sich mit Cybersecurity nachhaltig auseinandersetzen."

Bedrohungen. Phishing, Malware und Ransomware bilden seit Jahren die häufigste Angriffsart von Kriminellen auf heimische Unternehmen. Derartige Angriffe finden 365 Tage im Jahr und 24 Stunden am Tag statt. In den vergangenen zwölf Monaten wurden zwei von drei heimischen Unternehmen Opfer eines Cyber-Angriffs – um fünf Prozent mehr, als im Vergleich zur Vorjahresstudie. Ein Angriff durch Phishing, Malware oder Ransomware bedeutet, dass sich die Angreifer die Neugierde und die Gutgläubigkeit von Mitarbeiterinnen und Mitarbeitern von Unternehmen zunutze machen.

Der Faktor Mensch spielt im Bereich der Cyber-Kriminalität eine wesentliche Rolle. Die Abgelenktheit der Mitarbeiterinnen und Mitarbeiter oder die Selbstüberschätzung, multitaskingfähig zu sein, führen häufig zu Fehlentscheidungen. Diese ermöglichen es den Kriminellen, Zugang zu einem Unternehmen zu bekommen. Kompromittierte E-Mail-Konten und der Identitätsdiebstahl entwickeln sich zur meist verwendeten

Fotos: Gernot Burkert, Redtenbacher/Kpmg



Phishing, Malware und Ransomware bilden seit Jahren die häufigsten Angriffsarten von Kriminellen auf heimische Unternehmen.

Taktik der Angreifer für eine erfolgreiche Phishing-Attacke. Über kompromittierte E-Mail-Konten werden Phishing-Mails an Benutzer in einem Unternehmen gesendet. Phishing E-Mails, die innerhalb eines Unternehmens weitergeleitet werden, entgehen eher der Prüfung durch „E-Mail-Gateways".

Eine weitere – wenn auch rückläufige – Methode der Cyber-Kriminellen ist der Einsatz von „Cryptolockern", einer speziellen Ransomware, mit der Kriminelle auf einem Computer Daten verschlüsseln. Die Opfer werden damit erpresst, dass sämtliche Daten auf dem Computer gelöscht werden, sollten sie nicht innerhalb einer bestimmten Zeit Lösegeld bezahlen – meist in der Kryptowährung Bitcoin.

Eine weitere Herausforderung, vor die Unternehmen gestellt werden, ist das Erkennen der Intention des jeweiligen Angriffs. Insbesondere dann, wenn die Ziele eines Angreifers Wirtschaftsspionage, Produktpiraterie oder Know-how-Diebstahl sind.

Am häufigsten wurden Unternehmen laut Studie innerhalb der letzten zwölf Monate durch interne Sicherheitssysteme wie beispielsweise Firewalls, „Intrusion-Prevention-Systeme (IPS)" oder durch „Security-Information and Event-Management" (SIEM) auf Cyber-Angriffe aufmerksam. Der wesentliche Hinweis auf einen Angriff kam dabei in 65 Prozent der Fälle von aufmerksamen Mitarbeiterinnen und Mitarbeitern. In seltenen Fällen kam die wichtige Information von externen Zulieferern, Medien oder Behörden.

Rasche Reaktion. Wesentlich bei Cyber-Angriffen ist es, rasch zu reagieren, um größere Schäden verhindern zu können. Laut Studie sind immer mehr österreichische Unternehmen in der Lage, mit Angriffen aus dem Cyberspace richtig umzugehen und Cyber-Angriffe erfolgreich abzuwehren. 59 Prozent jener Unternehmen entstand kein Schaden, die innerhalb der letzten zwölf Monate Opfer eines Cyber-Angriffs wurden.

Vorfälle anzeigen. Ein weiterer wesentlicher Punkt ist eine Dokumentation von Cyber-Vorfällen und Cyber-Angriffen, sowohl für die Allgemeinheit wie auch für andere Unternehmen. Dazu zählt die Anzeige des Vorfalls an die Sicherheitsbehörde.

Laut Studie wenden sich nur rund 33 Prozent der betroffenen Unternehmen an die Behörden, bei denen Sicherheitsvorfälle stattfanden. Nur rund ein Viertel jener Unternehmen, die einen Schaden durch einen Cyber-Angriff erlitten, wandte sich an die Polizei. Anzeigen der Vorfälle sind für die Behörden und deren Kampf gegen die Internetkriminalität von Bedeutung. Würden Unternehmen den Behörden derartige Vorfälle konsequent melden, könnte ein klareres Cyber-Kriminalitäts-Lagebild für den Wirtschaftsstandort Österreich gezeichnet werden. Die Expertinnen und Experten der Polizei wären in der Lage, bessere Unterstützungsmöglichkeiten für Unternehmen zu schaffen.

Das Netz- und Informationssystemsicherheitsgesetz (NISG) soll Unternehmen sensibilisieren, derartige Vorfälle und Angriffe zu melden. Vor allem große Unternehmen haben laut Studie bereits in den vergangenen zwölf Monaten vorbildlich gehandelt. Das NISG verpflichtet bestimmte Unternehmen – Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung – zur Errichtung umfangreicher Cyber-Sicherheitsmaßnahmen und verlangt den Nachweis, dass diese Maßnahmen auch Wirkung zeigen. „Staatliche Stellen, sowie Aufsicht und Regulatoren lassen dieser Materie eine ganz besondere Wichtigkeit zukommen. Bei Nichteinhaltung der Anforderungen aus dem NISG drohen Strafen und ein Reputationsverlust", erläuterte Lamprecht. (Genaue Ausführungen zum NISG finden sich im Artikel „Mehr Netz- und Informationssicherheit durch klare gesetzliche Regelungen in dieser Ausgabe").

Aufgabe des Managements. Der technologische Wandel und die Digitalisierung machen neue Cybersecurity-Strategien notwendig. Erforderlich sind umfassende technologische und organisatorische Lösungen. Diese Lösungen müssen den „Faktor Mensch" berücksichtigen und das Unternehmen widerstandsfähig gegen Cyber-Angriffe machen. Die Studie stellt klar, dass es im Kampf gegen die Cyber-Kriminalität in Unternehmen von entscheidender Bedeutung ist, welche Rolle die Cyber-Sicherheit aus Sicht der Führungsebene in einem Unternehmen einnimmt.

Cybersecurity ist eine Aufgabe des Managements. Diese Aufgabe muss demnach „top-down" organisiert und umgesetzt werden. Wesentliche und entscheidende Faktoren dabei sind eine offene Kommunikation und eine positive Kultur im Umgang mit dem Thema. Laut der Studie kann der Cyber-Kriminalität nur durch integriertes Securitymanagement begegnet werden.

Die Cyber-Security-Studie ist downloadbar unter *https://home.kpmg/at/de/home.html* *Gernot Burkert*

FOTO: ANDREY POPOV/STOCK.ADOBE.COM