CYBER SECURITY TRENDS UND EMPFEHLUNGEN 2019

CYBER SECURITY TRENDS 2019

Angriffe auf geschäftliche E-Mail-Kommunikation nehmen zu (Business E-Mail Compromise bzw. Spear-Phishing-Angriffe)
Das Kommunikationsmedium E-Mail ist ein beliebtes Hilfsmittel für Angreifer, vor allem bei Phishing- und anderen Social-Engineering-Angriffen auf Unternehmen. Die Opfer werden zur Bekanntgabe sensibler interner Informationen oder zum Bezahlen von gefälschten Rechnungen verleitet. Dies betrifft insbesondere Führungskräfte (CEOs, CFOs etc.) und Mitarbeiterinnen und Mitarbeiter der Buchhaltung und des Rechnungswesens.

Erpressungsvorfälle durch Ransomware häufen sich
Erpressungsvorfälle durch Ransomware wie z.B. WannaCry stiegen 2018 um bis zu 350% im Vergleich zum Vorjahr, wobei der Gesundheitssektor immer stärker in den Fokus der Angreifer rückt. Das Ziel ist immer das Gleiche: Informationen stehlen bzw. verschlüsseln, um anschließend Geld - meist in Form von Kryptowährungen - zu erpressen.

Steigende (internationale) Compliance-Anforderungen
Unternehmen müssen sich laufend mit neuen Gesetzen, Verordnungen und Richtlinien in den Bereichen Informationssicherheit und Datenschutz auseinandersetzen (DSGVO, NIS-RL, ePrivacy-VO). Aufgrund der strengeren und komplexeren regulativen Anforderungen müssen künftig mehr Maßnahmen ergriffen werden. Damit steigt in diesen Bereichen der Bedarf an Expertinnen und Experten.

Fachkräftemangel in der Informationssicherheitsbranche
Der Mangel an Cybersecurity-Expertinnen und Experten stellt Unternehmen auch im Jahr 2019 vor Herausforderungen. Erfahrene, ausgebildete und zertifizierte Fachkräfte im Bereich Cybersecurity sind Mangelware.

Resignation in Bezug auf Informationssicherheit
Die Konsolidierung vieler Daten in den Händen einiger weniger Unternehmen, zunehmende Abhängigkeit von vernetzten Geräten (IoT) und ständige Meldungen zu Onlinebedrohungen und Datenschutzverletzungen haben die Bevölkerung desensibilisiert. Viele Personen resignieren und geben die Kontrolle über ihre digitale Präsenz auf (Leitsatz: „Ich habe nichts zu verbergen"). Dies hat zur Folge, dass sich potenzielle Angreifer diese Bequemlichkeit zunutze machen und Delikte wie Identitätsdiebstahl bzw. Internetspionage deutlich zunehmen.

Schwachstellen bei Geschäftspartnern gefährden das eigene Netzwerk
Schnittstellen für Geschäftspartner (z.B. VPN, Kundenportale etc.) werden oftmals von Angreifern genutzt, um Zugriff auf sensible Unternehmensdaten zu erlangen. Dazu verschaffen sie sich Zugang zum Netzwerk des Geschäftspartners und dringen anschließend über die Schnittstellen in das eigentliche Zielunternehmen vor. Die Schnittstellen sind aufgrund des Vertrauensverhältnisses zwischen Geschäftspartnern häufig weniger gut abgesichert bzw. überwacht, weshalb Angriffe nicht schnell genug erkannt werden.

Informationssicherheitsstandards im Fokus der Unternehmen
Neben dem Aufbau eines prozessorientierten Informationssicherheits-Managementsystems nach international anerkannten Standards wie ISO/IEC 27001 stehen die Identifizierung und angemessene Umsetzung von konkreten Maßnahmen im Vordergrund der Unternehmen. Um auch die Wirksamkeit der Maßnahmen feststellen zu können, gewinnen regelmäßige Analysen, organisatorische und technische Sicherheitsüberprüfungen, sowie Szenarien basierte Notfallübungen immer mehr an Bedeutung.

CYBER SECURITY EMPFEHLUNGEN 2019

Regelmäßig E-Mail-Threat-Analyse durchführen!
In den letzten Jahren wurden viele Methoden und Tools zur Erkennung und Abwehr von Betrugsversuchen entwickelt bzw. verbessert. Viele Maßnahmen sind bereits in den meisten Unternehmen implementiert (z.B. Virenschutz, DKIM, SPF etc.). Um deren Wirksamkeit zu testen, empfiehlt sich die periodische Durchführung einer E-Mail-Threat-Analyse. Dabei wird gezielt versucht, die Sicherheitsmaßnahmen zu umgehen und Malware einzuschleusen.

Effektives und zeitgerechtes Patch Management umsetzen!
Angreifer nutzen Schwachstellen in veralteten, nicht aktualisierten Systemen, um sich unautorisiert Zugang zu Unternehmensdaten zu verschaffen. Effektive Patch Management Programme und das zeitgerechte Schließen von aufgetretenen Schwachstellen können solche Angriffe verhindern.

Cybersecurity-Bewusstsein durch Awareness-Schulungen und -Trainings steigern!
Der Mensch rückt bei Social-Engineering -Angriffen in den Fokus der Angreifer, weshalb technische Maßnahmen hier keinen ausreichenden Schutz bieten. Zur Vorbeugung sollten Maßnahmen wie z.B. simulierte Phishing-Kampagnen und Schulungen zur Steigerung des Cybersecurity-Bewusstseins ergriffen werden.

Incident-Management-Prozess implementieren!
Werden Incident Response- und Business Continuity Pläne ausgearbeitet, so können Unternehmen angemessen auf Informationssicherheitsereignisse reagieren. Das Incident-Management sollte unternehmensweit als zentrale Stelle agieren und als Schnittstelle zu den lokalen Behörden (z.B. Datenschutzbehörde) fungieren. Mithilfe von Cybersecurity-Simulationen können Unternehmen und Belegschaft auf den Ernstfall vorbereitet werden.

Ganzheitliche Strategie zur Überwachung der IT-Infrastruktur entwickeln!
Zur Identifikation und Reaktion auf potenzielle Bedrohungen müssen Technologien zur Überwachung der IT-Infrastruktur implementiert werden. Dazu sollte eine organisationsweite Strategie hinsichtlich Monitoring und Log-Management entwickelt werden.

Regelmäßig Effektivitätsprüfungen durchführen!
Sämtliche Richtlinien, Prozesse, Checklisten und andere Dokumentation sollten in regelmäßigen Abständen auf Vollständigkeit, Angemessenheit und Effektivität überprüft werden. Getroffene organisatorische und technische Maßnahmen sollten stets der vorherrschenden Bedrohungslage entsprechen und durch regelmäßige Risikoanalysen validiert werden.

Sicheres Benutzer- und Zugriffsmanagement etablieren!
Neben der Verwendung von starken Passwörtern ist es unerlässlich, ein Konzept zur Verwaltung und Vergabe von Berechtigungen zu etablieren. Der Einsatz von privilegierten Benutzerkonten (Administratoren) soll auf ein Minimum beschränkt werden. Zur Vergabe von Berechtigungen sollte ein simples wie auch effizientes Konzept erstellt werden, das einfach gewartet und auditiert werden kann. Zieht man zuletzt veröffentlichte Data Breaches und Passwortdatenbanken (z.B. Collection #1) zu Rate, so sollten Unternehmen den Einsatz von Mehrfaktorauthentifizierung mithilfe von (Hardware)-Tokens bzw. Biometrie (z.B. Fingerabdruck) evaluieren.

Netzwerk- und Applikationsinfrastruktur überprüfen!
Regelmäßige automatisierte Überprüfungen der Netzwerkinfrastruktur identifizieren etwaige vorhandene Schwachstellen. Besonders kritische Systeme sollten zusätzlich einer sorgfältigen technischen Sicherheitsüberprüfung (Penetration Test) unterzogen werden.

ZUSAMMENFASSUNG

Cybersecurity-Vorfälle schädigen ein Unternehmen nachhaltig. Während finanzielle Verluste durch Versicherungen abgedeckt werden, ist der Reputationsschaden oft irreparabel. Ist das Vertrauen der Kunden und Geschäftspartner verloren, kann es nur sehr schwer wiedergewonnen werden. Steigt das Know-how im Unternehmen, steigen auch Unternehmenswert und Reputation. Unternehmen müssen sich zu jeder Zeit bewusst sein, welche Daten bzw. Informationen sie verarbeiten und welchen Wert diese Informationen besitzen. Nur dann können wirksame Maßnahmen getroffen werden, um Unternehmenswerte zu schützen und regulative Anforderungen zu erfüllen.

In Zeiten der Digitalisierung und Compliance-Anforderungen wie der DSGVO muss der Schutz von Daten und Informationen oberste Priorität für Unternehmen haben. Investitionen in die Informationssicherheit reduzieren die Wahrscheinlichkeit von Datenschutz- und Informationssicherheitsvorfällen und beugen somit auch Reputationsverlust, Lösegeldzahlungen und möglichen Strafen vor. Langfristig steigert gelebte Informationssicherheit nicht nur das Vertrauen der Kunden, sie führt mit der IT-Abteilung als Business Enabler zum Geschäftserfolg des Unternehmens.

KONTAKT

EWALD KAGER
Partner
IT & Risk Advisory
+43 732 27 29 75
ewald.kager@bdo.at

ROLAND PUCHER
Senior Manager
Cyber Security & Digital Forensics
+43 732 27 29 75
roland.pucher@bdo.at