Tipp 1: Cyber-Sicherheit ist Chefsache!
Wer von der Digitalisierung profitieren will, muss Informationssicherheit als dafür unabdingbare Voraussetzung verstehen und umsetzen. Informationssicherheit ist ein strategisches Thema und damit eine Leitungsaufgabe für das Topmanagement.

Tipp 2: Cyber-Resilienz erhöhen!
Bereiten Sie Ihr Unternehmen auf mögliche Vorfälle vor. Halten Sie Übungen ab, spielen Sie regelmäßig neue Szenarien durch. Setzen Sie Krisenreaktionsmechanismen auf: Wer darf entscheiden, ob der Webserver heruntergefahren wird? Welche Netzwerksegmente dürfen offline gestellt werden? Wer ist im Notfall außerhalb der Bürozeiten erreichbar, auch ohne funktionierendes Netzwerk? Wer ist befugt, Entscheidungen zu treffen?

Tipp 3: Netzwerke schützen Netzwerke!
Der Austausch zu Bedrohungen und vorbildlichen Absicherungen über die Unternehmensgrenzen hinweg ist ein wichtiger Baustein, um zielführende Schutzmaßnahmen zu etablieren. Werden Sie Mitglied im UP KRITIS, der öffentlich-privaten Kooperation der Betreiber Kritischer Infrastrukturen mit den zuständigen staatlichen Stellen, oder in der Allianz für Cyber-Sicherheit, den Plattformen des BSI für Information und Austausch.

Tipp 4: Managen Sie Cyber-Risiken!
Machen Sie kontinuierliche Bestandsaufnahmen der konkreten Bedrohungslage Ihres Unternehmens und setzen Sie entsprechende technische, organisatorische und prozessuale Schutzmaßnahmen um.

Tipp 5: Schützen Sie die „Kronjuwelen“!
Nicht alle Daten sind gleich wichtig oder für den Unternehmenserfolg entscheidend. Erstellen Sie ein Inventar der in Ihrem Unternehmen vorhandenen Daten und klassifizieren Sie diese nach Wichtigkeit. Die wertvollsten Daten sollten auch den höchsten Schutz genießen.

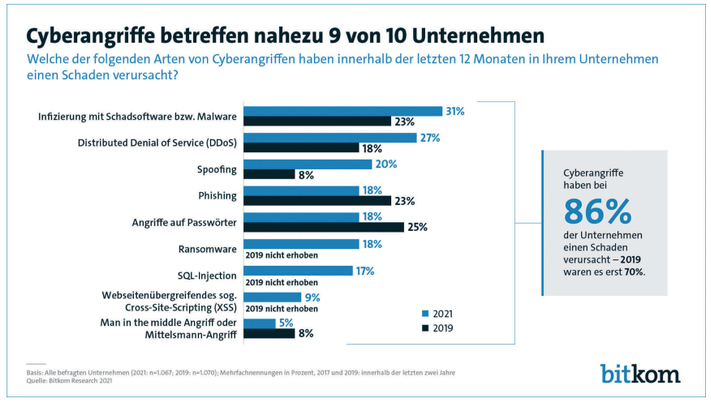
Tipp 6: Sichern Sie Ihre Daten!
Legen Sie Sicherungskopien, so genannte Backups, an und testen Sie diese. Cyberangriffe mit Erpressungssoftware (sogenannte Ransomware) sind für Cyber-Kriminelle ein einträgliches Geschäftsmodell, das Unternehmen an den Rand ihrer Existenz bringen kann. Wer seine Daten sichert, kann nicht erpresst werden. Backups sollten regelmäßig angelegt und regelmäßig auf Funktionalität, Konsistenz und Aktualität getestet werden.

Tipp 7: Die Mitarbeiter mitnehmen und regelmäßig schulen!
Cyber-Sicherheit zu realisieren heißt auch, dass Abläufe komplexer werden können. Zudem können auch Mitarbeiter Ziel von Cyber-Angriffen sein. Daher ist die Sensibilisierung und die regelmäßige Schulung der Mitarbeiter durch interne Awareness-Kampagnen zu aktuellen IT-Sicherheitsthemen oder Angriffsmethoden ein wichtiger Baustein der Cyber-Sicherheit.

Tipp 8: Patchen, patchen, patchen!
Verschaffen Sie sich einen Überblick über die im Unternehmen eingesetzte Hard- und Software und sorgen Sie dafür, dass von den Herstellern bereitgestellte Sicherheitsupdates schnellst möglich eingespielt werden. Wenn die Software/Firmware auf dem neuesten Stand ist, ist das Risiko eines erfolgreichen Cyber-Angriffs signifikant geringer.

Tipp 9: Verschlüsselung sollte der Normalfall werden!
Denn Verschlüsselung schützt vor Informationsabfluss. Der durchgehende Einsatz sicherer Kryptografie darf in Deutschland nicht mehr die Ausnahme sein, sondern sollte der Normalfall werden.

Tipp 10: Nutzen Sie die Angebote des BSI!
IT-Sicherheit in einem Unternehmen zu etablieren und nachhaltig sicherzustellen, ist eine komplexe Aufgabe. Hierbei gibt Ihnen das BSI als nationale Cyber-Sicherheitsbehörde Hilfestellung: Unter www.bsi.bund.de finden Sie Informationen zu Standards und Initiativen, Lageberichte und Empfehlungen sowie eine Fülle vertiefender Publikationen. Als Teilnehmer der Allianz für Cyber-Sicherheit profitieren Sie darüber hinaus vom persönlichen Dialog mit Experten und anderen Anwendern aus der Wirtschaft. ■



Schäden durch Cyberangriffe
Neun von zehn Unternehmen waren 2020/2021 von Cyberangriffen betroffen. Insgesamt verursachten die folgenden Arten von Cyberangriffen Schäden in den Unternehmen (Mehrfachantworten waren möglich), wie der Digitalverband Bitkom in einer repräsentativen Studie aufzeigte.

Das BSI hat auf seiner Webseite ein umfangreiches Cyber-Glossar veröffentlicht. Die vom Digitalverband Bitkom benannten Schäden durch Cyberangriffe erläutert Zahntechnik TELESKOP in Kürze. Das komplette Cyber-Glossar finden Interessierte unter: www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html

Malware
Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus „Malicious software” und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde.

DOS / DDoS-Angriffe
Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service).

Spoofing [engl.]
Spoofing (von to spoof, zu deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten.

Phishing
Das Wort setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird z.B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen.

Ransomware
Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „ransom“) wieder freigeben.

Injection-Angriffe
Eine SQL-Injection-Schwachstelle gibt einem Angreifer die Möglichkeit, Datenbankabfragen über eine Applikation so zu manipulieren, dass der für den Angreifer interessante Teil einer Datenbank zurückgegeben wird, anstatt des Teils, der ursprünglich für die Anwendung vorgesehen ist. Unter Umständen können durch SQL-Injection auch Änderungen an den Datenbank-Inhalten vorgenommen oder sogar Programmcode ausgeführt werden.

Cross-Site Scripting (XSS)
Cross-Site-Scripting-Schwachstellen entstehen, wenn Benutzereingaben in einer Webanwendung ungefiltert durch den Server verarbeitet und an andere Clients zurückgegeben werden. Ein Angreifer hat damit unter Umständen die Möglichkeit, Programmcode wie JavaScript im Kontext des Benutzers einer Webseite auszuführen. Dies lässt sich unter anderem ausnutzen, um den Inhalt von Webseiten für einen Benutzer zu ändern oder auf Inhalte wie Cookies zugreifen zu können, um an Session-Informationen zu gelangen.

Man-In-The-Middle-Angriff
Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte” der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. ■