3 Wie Cyberattacken Datenpannen auslösen

Kaum jemand bezweifelt noch, dass Cyberattacken zu den größten Bedrohungen für Unternehmen gerechnet werden müssen, denn die fortschreitende Digitalisierung öffnet die Unternehmen für Angriffe aus dem Cyberraum. Doch viele Unternehmen sehen die Cyberangriffe eher als Auslöser für eine Betriebsunterbrechung. Tatsächlich sind die produktiven Prozesse eines Unternehmens in Gefahr, aber auch die personenbezogenen Daten. Genau genommen hängen die Betriebsunterbrechungen und die Verletzungen des Datenschutzes meist zusammen.

Im Folgenden werden Cyberattacken genauer betrachtet und ihre Bedeutung für das Eintreten einer Datenpanne untersucht. Zudem wird dargelegt, wie die Cybersicherheit dabei helfen kann, Datenpannen zu verhindern oder einzudämmen.

3/1 Wie Cyberattacken ablaufen

Bei dem Begriff „Cyberattacke" entstehen vor dem geistigen Auge in der Regel zwei Bilder: Zum einen ein Hacker, der mit einem Kapuzen-Pulli bekleidet seine Computertastatur wie eine Waffe nutzt. Zum anderen Schadsoftware (Malware), die sich ein Internetnutzer oder eine Internetnutzerin einfängt und die auf dem Computer Schaden anrichtet.

Beide Bilder sind zu einseitig, denn Cyberattacken sind sehr vielschichtig, wodurch ihre Erkennung, Abwehr und Eindämmung so schwierig wird. Weder der Angreifende noch das „Tatwerkzeug" sind so (einfach), wie man es sich gern vorstellt.

Die richtige Vorstellung ist aber entscheidend, damit die Cybersicherheit nicht zu einseitig geplant wird und letztlich nur eine Scheinsicherheit erreicht werden kann.

3/1.1 Vielfältige Angriffswege und -methoden

Tatwerkzeug Schadsoftware

In den nächsten Kapiteln wird noch näher dargestellt, welche Cyberattacken besonders bedrohlich für Unternehmen sind. An dieser Stelle soll stellvertretend für die weiteren Angriffskategorien betrachtet werden, dass es bereits auf der Ebene einer einzelnen Angriffskategorie wie Schadsoftware eine Vielzahl von Angriffswegen und Angriffsmethoden gibt.

Malware ist nicht gleich Malware

Unter einer Schadsoftware versteht man jede Software, die einer IT-Infrastruktur (Netzwerk, Hardware, Software, Daten) Schaden zufügen kann. Die für Schadsoftware gebräuchliche Bezeichnung Malware besteht aus dem ersten bzw. letzten Teil der englischen Wörter „malicious" (bösartig) und „software".

Schadsoftware ist keine fehlerhafte Software, die einen Schaden anrichtet, sondern der Schaden wird ganz bewusst verursacht. Ziele der Programmierer und Verbreiter von Schadprogrammen können die Zerstörung, Manipulation oder Blockade von IT-Systemen sowie die Löschung, die Manipulation oder das Ausspähen von Daten sein.

BEISPIEL

Schadsoftware kommt in unterschiedlichen Varianten vor, von denen jeweils verschiedene Gefahrenpotenziale ausgehen und die unterschiedliche Angriffswege und -methoden nutzen:

- **Backdoor:**
  geheime Hintertür in den Computer für unerlaubte Fernzugriffe und eine heimliche Fernkontrolle
- **Boot-Virus:**
  Virus, der bereits beim Startvorgang des Computers (Boot) aktiviert wird
- **Bot:**
  bildet ein Netz aus ferngesteuerten, verseuchten Computern, die für kriminelle Zwecke missbraucht werden, zum Beispiel als heimliche Spam-Versender ohne Wissen und Zutun der Computernutzer
- **Datei- oder Programm-Virus:**
  Virus, der sich an eine Datei oder ein Programm anhängt, um aktiviert zu werden
- **Keylogger:**
  Schadsoftware, die alle Tastatureingaben mitschreibt und übermittelt, um insbesondere Passwörter zu stehlen
- **Makro-Virus:**
  Virus, der die Makrosprache z.B. in Office-Programmen ausnutzt
- **Polymorphe Viren:**
  Viren, die sich selbst verändern können, um nicht so leicht erkannt zu werden
- **RAM-Scraper:**
  Schadsoftware, die den Arbeitsspeicher (RAM) ausliest, in dem z.B. temporär entschlüsselte Daten liegen können
- **Ransomware:**
  Schadsoftware, die Dokumente unerlaubt verschlüsselt und Lösegeld für die Entschlüsselung erpressen will
- **Rootkit:**
  Programm, das dabei hilft, Schadsoftware besser zu verstecken (Tarnkappe für andere Malware)
- **Spyware:**
  Spionagesoftware zur Sammlung vertraulicher Daten

BEISPIEL

- **Trojaner oder Trojanisches Pferd:**
  scheinbar nützliches Programm, das eine bösartige Funktion in sich trägt
- **Würmer:**
  Schadsoftware, die sich selbst vervielfältigen kann, ohne andere Dateien zu infizieren, und sich zum Beispiel selbsttätig über E-Mail-Programme ausbreitet

Malware verbreitet sich auf vielen Wegen

Schadsoftware wird meist mit dem Internet in Verbindung gebracht. Tatsächlich ist das Internet einer der Hauptverbreitungswege für Malware. Doch auch IT-Systeme ohne Internetverbindung können von Schadprogrammen befallen werden.

Verbreitung im Internet

Der bei den Internetnutzenden bekannteste Verbreitungsweg für Schadsoftware ist die E-Mail. Dabei ist nicht der E-Mail-Text selbst das Schadprogramm, sondern ein Hyperlink (Internetverknüpfung) im E-Mail-Text führt beim Anklicken zum Herunterladen eines Schadprogramms. Alternativ befindet sich das Schadprogramm bei verseuchten E-Mails im Dateianhang. Potenziell gefährlich sind dabei nicht nur Programmdateien (Dateiendung *.exe), sondern jedes Dateiformat kann ein getarntes Schadprogramm sein, also auch Office-Dateien, Bilddateien, PDF-Dateien, um nur einige Beispiele zu nennen.

Neben der Verbreitung von Malware über E-Mails können Schadprogramme auch in Webinhalten versteckt sein, die mit dem Browser oder einer Browsererweiterung (Plug-in) geöffnet werden, also Webseiten, Bilder, Online-Videos oder Musikdateien. Dabei ist es nicht erforderlich, dass der verseuchte Hyperlink oder Webinhalt aktiv angeklickt wird. Bereits das Öffnen einer Webseite, die mit Schadprogrammen verseuchte Inhalte aufweist, kann zu einer Malware-Infektion führen. Man spricht deshalb von Drive-by-Downloads, also dem Herunterladen von Schadprogrammen im „Vorbeifahren". Nicht nur von unseriösen oder illegalen Webinhalten geht ein solches Risiko aus. Jede unzureichend abgesicherte Webseite kann manipuliert und mit Malware versehen werden.

Neben E-Mail und World Wide Web (WWW) sind auch alle anderen Internetdienste mögliche Verbreitungswege für Malware, zum Beispiel FTP (File Transfer Protocol), P2P (Peer-to-Peer-Dienste wie Tauschplattformen im Internet), VoIP (Voice-over-IP, Internettelefonie), Chat-Dienste, Instant Messaging (Echtzeit-Kommunikation im Internet) und soziale Netzwerke mit ihren Kommunikationsdiensten.

Verbreitung außerhalb des Internets

IT-Systeme sind immer dann von Schadprogrammen bedroht, wenn ein Systemzugriff wie z.B. ein Datenaustausch stattfindet, wenn also neue Dateien auf das IT-System gelangen können. Für einen solchen Systemzugriff ist kein Internet erforderlich, vielmehr können die Schadprogramme über jede Systemschnittstelle oder Netzwerkverbindung auf das IT-System gelangen.

Schadprogramme können also auch über optische Medien wie CDs/DVDs (via optisches Laufwerk) übertragen werden, über USB-Sticks und andere USB-Speichermedien (via USB-Schnittstelle), aber auch über eine lokale Funkverbindung (wie Wireless Local Area Network (WLAN), Bluetooth, NFC (Near Field Communication) oder Infrarot-Kurzstreckenverbindung). Malware kann auch über die interne Netzwerkverbindung (LAN, Local Area Network) des Unternehmens übertragen werden, wenn es keine Internetzugänge an den Arbeitsplätzen gibt. Selbst bei Anschluss einer Computermaus, einer Tastatur oder eines Druckers könnten Schadprogramme auf den Rechner gelangen, wenn die angeschlossenen Geräte zuvor mit Schadprogrammen infiziert wurden.

Viele interessante Zielsysteme: Nicht nur PCs sind betroffen

Die Verbreitungswege für Schadprogramme sind ebenso vielfältig wie die möglichen Zielsysteme. Personal Computer unter einem Windows-Betriebssystem sind wegen ihrer hohen Verbreitung besonders häufig in den Schlagzeilen, wenn es um Malware-Attacken geht. Generell von Schadsoftware bedroht sind allerdings alle IT-Systeme, unabhängig vom Betriebssystem. Sobald ein IT-System eine gewisse Verbreitung auf dem Markt erreicht hat, wird es für die Entwickler und Verbreiter von Schadsoftware zum interessanten Zielsystem.

Neben den Windows-PCs können also z.B. auch Apple-Rechner mit Mac-Betriebssystem, Linux-Rechner, Serversysteme sowie Tablets, Smartphones und Handys mit Malware infiziert werden. Auch Netzwerkkomponenten wie Router können befallen werden, im Prinzip jedes System, das softwarebasierte Befehle ausführen kann. Dazu gehören auch die vernetzten Geräte im Smart Home, die vernetzten Industrieanlagen (Industrie 4.0) oder allgemein das Internet of Things (IoT, Internet der Dinge).

3/1.2 Die Vielfalt der Tätergruppen

Täter sind nicht nur die „Hacker"

Nicht nur die Angriffsmethoden, Angriffswege und Angriffswerkzeuge sind sehr vielfältig, auch die Täterkreise sind vielschichtig.

BEISPIEL

So ergab zum Beispiel eine Umfrage zum Wirtschaftsschutz 2021 des Digitalverbands Bitkom (Mehrfachnennungen möglich):

- In 61 % der von Diebstahl, Spionage und Sabotage betroffenen Unternehmen wurden Schäden durch **Mitarbeiterinnen und Mitarbeiter** verursacht, teils auch nachdem sie bereits aus dem betroffenen Unternehmen ausgeschieden waren. 42 % der betroffenen Unternehmen berichten von Mitarbeiterinnen und Mitarbeitern, die **unabsichtlich** gehandelt haben. 28 % der Unternehmen gehen dagegen davon aus, dass Schäden **vorsätzlich** herbeigeführt wurden. Eine unzureichend geschulte oder unaufmerksame Belegschaft und Innentäter bleiben damit ein zentrales Problem für die deutsche Wirtschaft. Viele Angriffe kommen aber von außen, beispielsweise von Privatpersonen bzw. **Hobby-Hackern** (40 %).
- Der stärkste Zuwachs im Vergleich zu den Vorjahren ist allerdings der **organisierten Kriminalität** zuzurechnen: In den Jahren 2016/2017 führten 7 % der betroffenen Unternehmen Attacken auf organisierte Kriminalität zurück, 2018/2019 bereits 21 %. 2020/2021 ist der Wert nun auf 29 % gestiegen.

Ein ähnliches Bild zeichnet die IT-Sicherheitsumfrage 2022 des Verbands der Internetwirtschaft eco. Auch dort sieht die Mehrzahl der befragten Sicherheitsexpertinnen und -experten die meisten Täter bei den „profitgetriebenen Cyberkriminellen".

Der Angriffsursprung: Nicht immer das Ausland

Die meisten Angriffe kommen aus Deutschland: 43 % der geschädigten Unternehmen vermuten die Täterinnen und Täter im Inland. 37 % geben an, die Handlungen wurden aus Osteuropa (ohne Russland) vorgenommen (2018/2019: 28 %). China (30 %) und Russland (23 %) wurden ebenfalls häufig als Ursprungsregionen identifiziert; seltener die USA (16 %). Indes konnten 31 % der Unternehmen keine Angaben machen, woher sie angegriffen wurden. Dieser Wert stieg im Vergleich zu den Jahren 2018/2019 um sieben Prozentpunkte – ein Indiz für erfolgreichere Verschleierungstaktiken der Angreifer.

WICHTIG

Um Cyberattacken so früh wie möglich zu erkennen und abzuwehren sowie die Folgeschäden wie Datenmissbrauch möglichst einzudämmen, ist es wichtig, die Vielfalt der Cyberattacken zu sehen, mit all ihren Angriffswegen, Angriffsverfahren, Angriffswerkzeugen und Tätergruppen. Entsprechend vielschichtig muss auch das Konzept der Cybersicherheit sein, um Datenpannen verhindern oder minimieren zu können.

Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2017 und 2019: innerhalb der letzten zwei Jahren) von Diebstahl, Industriespionage betroffen waren (2021: n = 935; 2019: n = 801; 2017: n = 571); Mehrfachnennungen in Prozent | Quelle: Bitkom Research 2021

Abb. 5: *Hinter vielen Cyberattacken steckt die organisierte Kriminalität, so eine Umfrage des Digitalverbands Bitkom (Bild: Bitkom)*

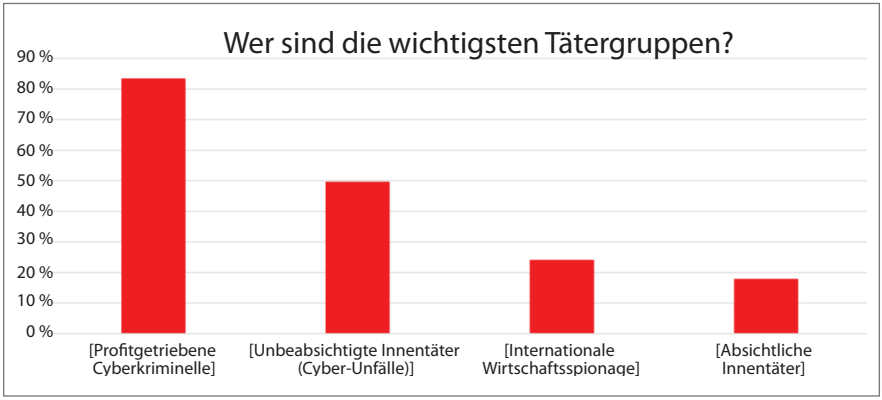

Abb. 6: *Der größte Täterkreis wird in den Cyberkriminellen gesehen, die kriminelle, finanzielle Ziele verfolgen, so auch die eco-Umfrage IT-Sicherheit 2022 (Bild: eco-Verband)*

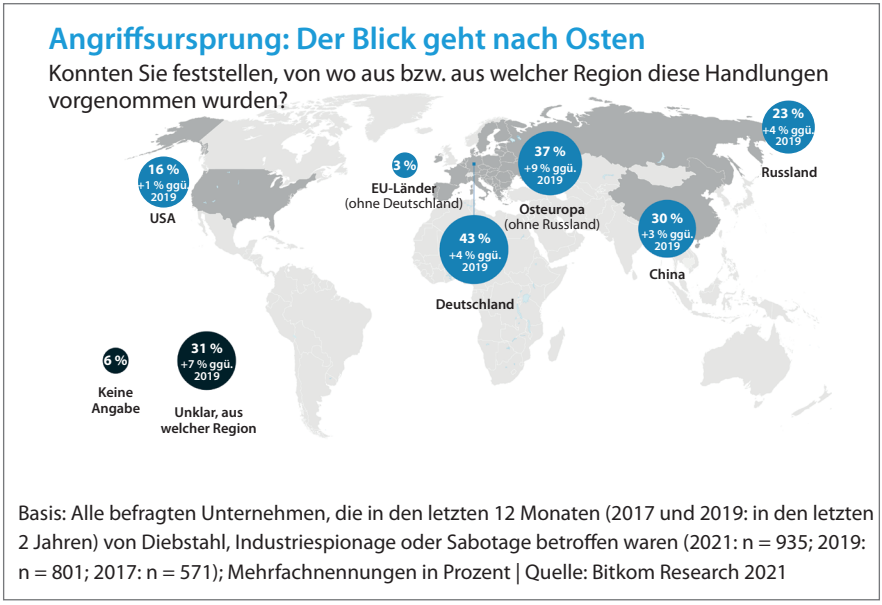

Abb. 7: *Die Angriffe kommen nicht nur von außerhalb, auch Innentäter gehören zu den möglichen Angreifern, wie eine Bitkom-Umfrage bestätigt (Bild: Bitkom)*

3/1.3 Die vielen Stufen einer Cyberattacke

Modell „MITRE ATT&CK" für den Ablauf einer Attacke

In der Cybersicherheit gibt es ein führendes Modell, das die einzelnen Schritte eines Cyberangriffs aufführt. Ein solches Modell hilft zum Beispiel bei der Entwicklung eines Konzepts der Cybersicherheit, da man entlang des Modells planen kann, wie man diese Phase der Attacke verhindern oder erkennen und die Folgen abmildern kann.

Selbst Hersteller für Cybersicherheitslösungen und Testinstitute verwenden das Modell MITRE ATT&CK (www.mitre.org), um eine Lösung möglichst genau mit ihren Funktionen und Leistungsparametern erfassen und einordnen zu können.

MITRE ATT&CK ist eine Wissensdatenbank, die von Netzwerkverteidigern häufig verwendet wird, wenn sie Sicherheitsbedrohungen analysieren und darüber berichten. Das Verständnis des gegnerischen Verhaltens ist oft ein entscheidender erster Schritt zum Schutz von Netzwerken und Daten, und der Erfolg, den Verteidiger beim Erkennen und Eindämmen von Cyberangriffen haben, hängt von diesem Verständnis ab. Ein solides Verständnis der Anwendung von ATT&CK kann zur Entwicklung von Profilen der Angreifenden verwendet werden, um Trendanalysen durchzuführen und die Berichterstattung zu Erkennungs-, Reaktions- und Minderungsmaßnahmen zu untermauern, so die Organisation MITRE.

Die Schritte eines Cyberangriffs

Die einzelnen Schritte einer Attacke nach dem MITRE ATT&CK Framework sind:

- **Schritt 1: Initiale Malware-Verseuchung**
  Eine Malware wird beim Opfer ausgebracht und ausgeführt, sie stellt heimlich die Verbindung zu dem Angreifenden her.
- **Schritt 2: Sammlung und Exfiltration**
  Der Angreifende führt einen Datendiebstahl durch, indem die Malware Daten einsammelt und versendet.

- **Schritt 3: Tarnung bereitstellen**
  Der Angreifende löscht die erste Malware, nutzt höhere Berechtigungen, die er erbeutet hat und stellt eine Verbindung nach extern her, um Daten auszuschleusen und eine Hintertür einzurichten.
- **Schritt 4: Aufräumen**
  Der Angreifende beseitigt Angriffsspuren und untersucht die weitere IT-Umgebung des Opfers.
- **Schritt 5: Persistenz herstellen**
  Der Angreifende richtet Wege für den dauerhaften Zugang zum Opfer ein.
- **Schritt 6: Zugriff auf Anmeldeinformationen**
  Der Angreifende sammelt verschiedene Formen von Anmeldeinformationen, die er erbeuten kann.
- **Schritt 7: Exfiltration**
  Der Angreifende sammelt weitere Daten des Opfers und schleust Daten aus.
- **Schritt 8: Zugriffe erweitern**
  Der Angreifende nutzt die erbeuteten Daten auf einem Remote-Computer aus.
- **Schritt 9: Bereinigen, Sammeln und Exfiltrieren**
  Der Angreifende setzt neue Tools ein, führt einen weiteren Datendiebstahl durch und bereinigt dann die Spuren auf dem Remote-Computer.
- **Schritt 10: Weitere Persistenz**
  Persistenzmechanismen (Verfahren für einen dauerhaften Zugang) werden ausgeführt, wenn der Computer des Opfers neu gestartet wird.
- **Schritt 11: Erneute Verseuchung des Systems**
  Neue Malware wird beim Opfer ausgeführt.
- **Schritt 12: Zugriff verstärken**
  Der Angreifende versucht wieder, Zugriffe zu erlangen und Spuren zu verbergen.
- **Schritt 13: Weitere Aufklärung**
  Der Angreifende untersucht mit weiteren Berechtigungen die IT-Umgebung des Opfers.
- **Schritt 14: Zugriff auf Anmeldeinformationen**
  Der Angreifende nutzt die höheren Berechtigungen und speichert weitere gestohlene Anmeldeinformationen.
- **Schritt 15: Persistenz herstellen**
  Der Angreifende richtet einen zweiten Weg für den dauerhaften Zugang zum Opfer ein.

- **Schritt 16: Erweiterung des Zugriffs**
  Der Angreifer speichert neue Anmeldeinformationen.
- **Schritt 17: Erfassung**
  Der Angreifer sammelt wieder Daten des Opfers und verschleiert den Angriff.
- **Schritt 18: Exfiltration**
  Der Angreifende schleust wieder die Daten aus.
- **Schritt 19: Aufräumen**
  Der Angreifende beseitigt wieder die Spuren.
- **Schritt 20: Persistenzausführung**
  Persistenzmechanismen werden wieder ausgeführt, wenn der Computer des Opfers neu gestartet wird. Das Ziel ist es, sich dauerhaft unerkannt einzunisten.

Auch wenn die genannten Schritte eines Cyberangriffs bereits recht detailliert aussehen mögen, fassen sie doch jeweils mehrere Teilschritte in sich zusammen. Dies macht deutlich, wie komplex eine Cyberattacke sein kann und entsprechend wie kompliziert der Schutz, die Erkennung, die Abwehr und die Eindämmung.

Cyberattacken bestehen nicht einfach nur aus dem Versand einer verseuchten E-Mail, sie bestehen aus vielen Schritten, deren Ziel es ist, immer mehr Daten einzusammeln, sie auszuschleusen, immer neue Berechtigungen und Anmeldedaten zu stehlen, erneut Daten zu erbeuten sowie einen dauerhaften, unerkannten Zugang einzurichten. Die Abwehr ist deshalb auch nicht mit nur einer einzelnen und temporären Maßnahme möglich, sie muss vielschichtig und dauerhaft sein.

3/2 Cyberattacken und die Schutzziele im Datenschutz

3/2.1 Cybersicherheit und die Grundsätze im Datenschutz

Cybersicherheit dient dem Schutz der Infrastrukturen, Systeme, Anwendungen und Daten im Cyberraum und damit auch dem Schutz der personenbezogenen Daten im Cyberraum. Dies wird auch deutlich, wenn man sich bestimmte Grundsätze für die Verarbeitung personenbezogener

Daten nach der Datenschutz-Grundverordnung (Art. 5 Abs. 1 Buchstabe f DSGVO) ansieht:

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Ebenso fordert die DSGVO in Art. 32 Abs. 1 für die Sicherheit der Verarbeitung personenbezogener Daten:

…

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

…

Cyberattacken versuchen aber, genau diese Schutzziele der Vertraulichkeit, Verfügbarkeit, Integrität, Belastbarkeit und Wiederherstellbarkeit zu unterlaufen.

Angriffe auf die Vertraulichkeit

Viele Cyberangriffe haben das Ziel, vertrauliche Daten auszuspähen und dann zu missbrauchen. Meist haben diese Daten direkten oder indirekten Personenbezug.

Ein Beispiel für eine solche Attacke ist das Ausbringen einer Spyware, also einer Spionagesoftware, die vertrauliche Daten mitschreiben kann oder eine ungeschützte Datenverbindung abhört.

Angriffe auf die Verfügbarkeit und Wiederherstellbarkeit

Ebenso haben viele Cyberattacken das Ziel, Daten unbrauchbar zu machen, sie zu löschen und zu zerstören. Damit die Daten nicht wiederhergestellt werden können, werden auch die Datensicherungen und damit die Backups angegriffen, um sie zu zerstören und unbrauchbar zu machen.

Ein Beispiel für eine solche Attacke ist die gegenwärtig dominierende Variante von Cyberangriffen mittels Erpresser-Malware, also mit Ransomware, die kriminell Daten und möglichst auch die Datensicherung verschlüsselt und damit nicht mehr verfügbar und wiederherstellbar macht.

Angriffe auf die Integrität

Nicht ganz so häufig sind gegenwärtig Cyberangriffe, die die Daten manipulieren sollen, die Daten also verfälschen. Dies kann zum Ziel haben, digitale Spuren zu verwischen, aber auch falsche Informationen zu verteilen.

Ein möglicher Angriff ist die Veränderung von Webinhalten, das sogenannte Website Defacement. Denkbar ist es, so gefälschte Informationen zu streuen, die die Opfer schädigen oder weitere Attacken vorbereiten, indem die Opfer zuerst verunsichert und falsch informiert werden.

Angriffe gegen die Belastbarkeit

Cyberangriffe, die die Systeme zur Datenverarbeitung überlasten, werden auch Überlastungsangriffe genannt. Meist sind es **DoS-Attacken** oder **DDoS-Attacken** (Denial-of-Service- oder Distributed-Denial-of-Service-Attacken).

Dabei überlasten Angreifende zum Beispiel Webserver mit Anfragen so, dass diese überfordert sind und den Dienst einstellen, wenn der Angriff Erfolg hat. Die Website, die dieser Webserver veröffentlicht, geht dann offline. Die Überlastung des Webservers macht es schwierig bis unmöglich, auf die Daten, die der Server verwaltet, zuzugreifen. Mangelnde Belastbarkeit der IT wirkt sich so auf die Verfügbarkeit der Daten aus.

Cyberattacken dienen somit vielfach genau dazu, die Schutzziele, die der Datenschutz nennt, auszuhebeln und die Daten ihrer Vertraulichkeit, Integrität und Verfügbarkeit sowie die Systeme ihrer Funktionalität zu berauben.

3/2.2 Cyberattacken führen zur Datenschutzverletzung

Wann der Datenschutz verletzt ist

Bekanntlich definiert die DSGVO die „Verletzung des Schutzes personenbezogener Daten" als „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden".

Wie Cyberattacken den Datenschutz verletzen

Offensichtlich versuchen Cyberattacken genau das, also die Vernichtung, den Verlust, die Veränderung, die unbefugte Offenlegung von beziehungsweise den unbefugten Zugang zu personenbezogenen Daten zu erreichen. Man könnte also sagen, das Ziel einer Cyberattacke ist die Verletzung des Datenschutzes. Doch die Motive der Angreifenden liegen anders, sie wollen in aller Regel Profit durch die Attacken und mit den Daten machen.

Deshalb ist es richtig, zu sagen, die Folge einer Cyberattacke ist in den meisten Fällen eine Datenschutzverletzung oder Datenpanne. Cybersicherheit hat also aus Sicht des Datenschutzes die Aufgabe, Datenpannen zu verhindern oder zumindest einzudämmen.

WICHTIG

3/2.3 Cyberattacken erkennen, Daten schützen

Die Phasen der Cybersicherheit

Auf den ersten Blick würde man meinen, der sogenannte Cyberschutz wäre die Antwort auf die Cyberattacken, die den Datenschutz bedrohen. Doch die Cybersicherheit kennt mehr Phasen als den Cyberschutz, auch Cyber Protection genannt. In dieser Phase geht es darum, die Cyberangriffe zu verhindern, sodass insbesondere die Daten nie in den Zugriff Unbefugter kommen.

Leider gibt es keine Cyber Protection, die wirklich umfassenden Schutz bietet. Vielmehr muss man davon ausgehen, dass es Cyberattacken gibt, die kriminellen Erfolg haben, die also den Schutz überwinden.

Deshalb müssen Maßnahmen für die Cybersicherheit getroffen werden, die erfolgreiche Attacken erkennen. Diese Phase der Cybersicherheit wird Detection genannt. Ebenso müssen als Antwort auf die erkannten Attacken Maßnahmen ergriffen werden, die zur Abwehr und zur Eindämmung der Folgeschäden dienen. Diese Phase bezeichnet man als Response. Damit die betroffenen Daten wieder verfügbar und die angegriffenen Systeme wieder funktionstüchtig sind, kommt die Phase Recovery hinzu, also die Wiederherstellung, wie sie auch die DSGVO explizit für die Sicherheit der Verarbeitung (Art. 32 DSGVO) fordert.

Man kann also sagen, dass alle Phasen der Cybersicherheit für den Datenschutz relevant sind, die Protection, die Detection, die Response und die Recovery. Dies ist wichtig für die Ausgestaltung eines Konzepts der Cybersicherheit, denn für alle Phasen müssen Maßnahmen und Lösungen gefunden werden.