Einführung

Bei den folgenden Vorfällen und Versäumnissen handelt es sich um eine Auswahl ohne Anspruch auf Vollständigkeit. Die Beschreibungen dienen ausschließlich der allgemeinen Einführung und der Information über das Themenfeld. Vorfälle können in der Praxis ähnlich ablaufen, aber auch einen sehr unterschiedlichen Verlauf nehmen.

Die beschriebenen häufigen Versäumnisse sind aus realen Vorfällen abgeleitet, bei denen KPMG bei der Aufarbeitung unterstützt hat. Weiterhin wurden Sie durch Informationen aus öffentlichen Quellen ergänzt. Aufgeführte Empfehlungen zur Vermeidung sind allgemeiner Natur und sollten in jedem Fall vor einer Umsetzung anhand der eigenen Strukturen und Prozesse geprüft und ggf. angepasst werden.

Häufig beobachtete Cybersicherheitsvorfälle der vergangenen Jahre sind:

1. Verschlüsselungstrojaner

Auch bekannt als „Ransomware“, „Cryptolocker“ oder „Encryption Ransomware“.

Beschreibung

Ransomware beschreibt Schadsoftware, die Daten verschlüsselt und androht, diese erst nach Zahlung einer Lösegeldforderung („Ransom“) wieder herauszugeben. Sie wird häufig über E-Mail-Nachrichten verschickt und unbeabsichtigt durch Nutzer zur Ausführung gebracht. Frühe Versionen des Schadsoftwaretyps ließen sich aufgrund von Programmierfehlern teilweise ohne Zahlung entschlüsseln. Dies ist nun meist nicht mehr möglich. Bei einem Befall hilft in der Regel nur die Wiederherstellung der Daten aus Datensicherungen.

Häufige Versäumnisse und wie man sie vermeidet

- Mitarbeiter wurden nicht über die Gefahr und das richtige Verhalten bei verdächtigen E-Mails oder Hyperlinks geschult.
    - Schulen Sie Ihre Mitarbeiter zu digitalen Bedrohungen. Wiederholen Sie die Schulung in regelmäßigen Abständen oder nutzen Sie Aufzeichnungen für permanent verfügbare Online-Schulungen.
- Der Schutz gegen Schadsoftware ist nicht umfassend und/oder nicht aktuell.
    - Stellen Sie sicher, dass auf allen Systemen ein Grundniveau an Schutzmaßnahmen aktiv ist (insbesondere Antivirensoftware). Achten Sie auf eine konstante Aktualisierung der Schutzmaßnahmen (insbesondere aktuelle Erkennungsmuster für Schadsoftware).
- Es liegen keine bzw. keine aktuellen Datensicherungen (Backups) vor.
    - Stellen Sie ein Datenschutz-Konzept auf das bestimmt, welche Daten wo, wie und wie lange aufbewahrt werden. Die Funktionalität von Backups sollte regelmäßig geprüft werden. Backups müssen selbst vor Cyberangriffen geschützt werden.
- Die Datensicherungen wurden nicht getestet (Wiederherstellung) und sind nicht oder nur mit großem Aufwand wiederherstellbar.
    - Testen Sie Backups in regelmäßigen Abständen auf Integrität. Spielen Sie zudem den Wiederherstellungsprozess durch, um mögliche Fallstricke im Voraus zu beheben.
- Die Ransomware greift gleichzeitig personenbezogenen Daten ab. Aufsichtsbehörden werden nicht informiert.
    - Achten Sie bei einem begründeten Verdacht auf einen Verlust datenschutzrelevanter Daten auf eine zeitnahe Information der Aufsichtsbehörden.

2. Datenleck

Auch bekannt als „Data Leakage“ oder „Datenverlust“.

Beschreibung

Es gibt viele Ursachen für einen ungewollten Abfluss von Unternehmensdaten. In manchen Fällen sind es Mitarbeiter, die interne Daten unbeabsichtigt oder auch mit Vorsatz weitergeben. In anderen Fällen ist der Datenverlust eine Folge eines Angriffs. Auch Dienstleister können der Ursprung eines Datenverlusts sein. Oft fällt der Verlust erst auf, wenn die Daten – oder die Tatsache, dass es einen Vorfall gegeben hat – bereits an die Öffentlichkeit gelangt sind.

Häufige Versäumnisse und wie man sie vermeidet

– Für die Organisation kritische Informationen wurden nicht vorab identifiziert.

    - Schaffen Sie ein Dateninventar Ihrer „Kronjuwelen“. Sorgen Sie dafür dass dokumentiert ist, wo diese Daten gespeichert und verarbeitet werden und welche Wege die Informationen bei einem Transfer nehmen. So kann der Ursprung und der Hergang eines Datenlecks identifiziert werden.

– Es gibt keine definierte Vorgehensweise für den Fall, dass ein Datenverlust auftritt.

    - Erstellen Sie einen Incident Response Plan (IRP). Stellen Sie sicher, dass im Ernstfall klar ist wie und durch wen die Folgen eines Vorfalls eingedämmt werden können. Sorgen Sie insbesondere für den Fall verlorener Daten von Kunden oder Geschäftspartnern dafür, dass eine angemessen Kommunikation vorbereitet ist.

3. Sabotage durch Innentäter

Auch bekannt als „Disgruntled Employee“.

Beschreibung

Durch Spionage, Sabotage und Korruption von Mitarbeitern kann einem Unternehmen großer Schaden entstehen. Neben klassischer Korruption gibt es mittlerweile auch versteckte Online-Marktplätze (Foren) für Insiderinformationen, bei denen Innentäter Unternehmensinformationen verkaufen können. Im Fall einer Sabotage kann es zu Betriebsunterbrechungen kommen, insbesondere wenn der Saboteur über weitreichende technische Berechtigungen verfügt.

Häufige Versäumnisse und wie man sie vermeidet

– Interne Prozesse erleichtern oder ermöglichen unternehmensschädigendes Handeln.
    - Implementieren Sie Funktionstrennungen und Sicherheitsmaßnahmen wie z. B. ein technisch erzwungenes Vier-Augen-Prinzip bei kritischen Aktivitäten.

– Das Benutzerverhalten wird nur unzureichend protokolliert. Nach einem Vorfall ist eine Untersuchung des Hergangs nicht mehr möglich.
    - Sorgen Sie für geeignete, möglichst fälschungsresistente Aufzeichnungen. Achten Sie bei der Ausgestaltung der Aufzeichnungen auf datenschutzrechtliche Vorgaben!

– Mitarbeiter werden durch Unwissenheit zu Tätern oder Komplizen.
    - Das Sicherheitsbewusstsein der Mitarbeiter sollte durch kontinuierliche Schulungen gestärkt werden.

4. Infektion mit Schadsoftware

Beschreibung

Schadsoftware gibt es in großer Vielfalt. Sie kann für einen Anwendungszweck maßgeschneidert und gezielt eingesetzt werden oder von eher generischer Natur sein. Mittlerweile gibt es auch kommerzielle Schadsoftwareprodukte, die von Cyberkriminellen mit variablem Funktionsumfang als Dienstleistung erworben werden können. Auf diese Art können selbst technisch wenig versierte Kriminelle erfolgreiche Angriffe durchführen und hohen Schaden anrichten.

Häufige Versäumnisse und wie man sie vermeidet

– Dem Unternehmen fehlt es an grundlegenden Sicherheitsmaßnahmen.

    - Etablieren Sie ein Informationssicherheits-Managementsystem (ISMS). Am Anfang muss kein Maximalstandard stehen, beginnen Sie stattdessen mit der Zuweisung von Verantwortlichkeiten und einer strukturierten Auseinandersetzung mit Ihrem spezifischen Risiko.

– Mitarbeiter kennen digitale Bedrohungen nicht und wissen nicht, wie sie sich sicher verhalten sollen.

    - Schulungen und Awareness-Maßnahmen beugen einer unbeabsichtigten Mithilfe durch falsche Verhalten vor. Mitarbeiter die Bedrohungen kennen, können diese im Ernstfall erkennen und melden.

– Die Unternehmens-IT verfügt nicht über das notwendige Wissen und ausreichende Ressourcen, um ein angemessenes Schutzniveau zu erreichen.

    - Investieren Sie in das Know-How Ihrer Mitarbeiter. Ziehen Sie zudem externe Experten zu Rate oder lagern Sie gezielt Aktivitäten aus bzw. verstärken Sie diese durch externe (abrufbare) Ressourcen.

5. Professioneller Angriff

Beschreibung

Sogenannte Advanced Persistent Threats (APTs) sind Gruppen von Angreifern, die aufgrund ihrer verhältnismäßig guten Fähigkeiten und ihrer Persistenz hohe Erfolgsraten beim Angriff auf Organisationen erreichen. Häufig haben es diese Gruppen auf Daten abgesehen, die sich zu Geld machen lassen. Dabei kann es sich um Kunden- und Zahlungsdaten, aber auch um geistiges Eigentum und Strategiedokumente für Industriespionage handeln. Teilweise wird unterstellt, dass diese Gruppen durch staatliche Akteure beauftragt oder zumindest durch diese gefördert oder geduldet werden.

Häufige Versäumnisse und wie man sie vermeidet

- Das Vorgehen professioneller Gruppen ist nicht bekannt und daher auch keine Vorbereitung vorhanden.
    - Informieren Sie sich über die Werkzeuge und das Vorgehen professioneller Angreifergruppen. Prüfen Sie, ob Ihr Sicherheitsniveau auch diese Tätergruppe abdeckt.
- Kritische Sicherheitsupdates wurden nicht installiert. Der Allgemeinheit bekannte Sicherheitslücken sind weiter offen und können durch Angreifer ausgenutzt werden.
    - Beziehen Sie Informationen zu (kritischen) Sicherheitslücken und sorgen Sie für zeitnahe Updates.
- Eigenentwicklungen oder Anpassungen an vorhandener Software haben Sicherheitslücken.
    - Schulen Sie Ihre Mitarbeiter in sicherer Softwareentwicklung und stellen Sie entsprechende Vorgaben auf. Lassen Sie Eigenentwicklungen auf Sicherheitsprobleme überprüfen (Penetrationstest).

6. Überlastungsangriff

Auch bekannt als „Denial of Service“ (DoS) oder „Distributed Denial of Service“ (DDoS).

Beschreibung

Bei einem Denial of Service-Angriff (DoS) versucht ein Angreifer die Verfügbarkeit von Daten, Systemen oder Netzwerken zu beeinträchtigen. DoS-Angriffe werden gerne mit Hilfe tausender kompromittierter Systeme durchgeführt, die unwillentlich in einem sogenannten „Botnetz“ zusammengeschalten sind. Der durch diese „Zombies“ generierte Netzverkehr überflutet z. B. beliebte Webservices oder Onlineshops und sorgt dafür, dass legitime Nutzer nur einen eingeschränkten oder keinen Zugriff mehr haben. Teilweise geht der Angriff mit einer Erpressung einher – erst nach Zahlung lassen die Angreifer von der Überlastung ab.

Häufige Versäumnisse und wie man sie vermeidet

- Die Systeme sind nicht ausreichend dimensioniert.
    - Wenn die verfügbaren Ressourcen bereits durch reguläre Lastspitzen ausgereizt sind, können selbst kleinere Überlastungsangriffe erfolgreich sein. Ihre IT-Systeme sollten flexibel skalierbar sein, um Lastspitzen abfangen zu können.
- Einfache Überlastungsangriffe können nicht analysiert werden, da kein Monitoring besteht.
    - Sollte ein Angriff identifizierbar von einem Host ausgehen, dann kann dieser mittels schnell erstellbarer Sperrlisten abgewendet werden. Die IT-Administration benötigt hierfür die richtigen Monitoring- und Analysewerkzeuge sowie das Know-How zu deren Bedienung.
- Systeme oder Netzwerke sind nicht gegen Überlastungsangriffe geschützt.
    - Kritische Systeme lassen sich präventiv auf einen DoS-Angriff vorbereiten. Zusätzlichen Schutz können der Internetprovider oder ein spezialisierter sogenannter „Scrubbing“-Dienstleister bieten.
- Der Überlastungsangriff dient nur der Ablenkung, weitere schadhafte Aktivitäten werden übersehen.
    - Prüfen Sie, ob der DoS-Angriff nur von einem anderen Angriff ablenken soll.

7. Verlust von Hardware

Beschreibung

Ein Verlust von Hardware kann jederzeit vorkommen. Eine beliebte Masche ist der Diebstahl von Laptops in Bahn und Bus. Aus dem Verlust der Hardware kann ein Verlust sensibler Unternehmensinformationen oder eine Erpressung mit abgegriffenen Daten werden.

Häufige Versäumnisse und wie man sie vermeidet

– Es gibt keine Verhaltensregeln für den sicheren Umgang mit IT-Hardware.

    - Stellen Sie Verhaltensregeln auf und schulen Sie Ihre Mitarbeiter. Stellen Sie beispielsweise Schlösser für mobile Geräte zur Verfügung und schreiben Sie die Nutzung vor.

– Datenträger (Festplatten, Wechselmedien) werden nicht konsequent verschlüsselt.

    - Verschlüsseln Sie kritische Systeme. Im Idealfall sind alle Systeme und Datenträger die Ihre Geschäftsräume verlassen - oder einfach aus diesen entwendet werden können – verschlüsselt.

– Mangelnde Sicherheit der Geschäftsräume ermöglicht einen Diebstahl von Hardware.

    - Schützen sie Server- und Geschäftsräume durch Zugangskontrollen. Besucher sollten im Unternehmen begleitet werden. Leicht zu entwendende Hardware sollte durch Drahtschlösser befestigt werden.

8. Datenschutzverstoß

Beschreibung

Bei einer Verletzung nationaler oder übergreifender Datenschutzgesetze können empfindliche Strafen drohen. Zudem können öffentlich bekanntgewordene Datenschutzverstöße einen Reputationsverlust zur Folge haben.

Häufige Versäumnisse und wie man sie vermeidet

- Mitarbeitern sind nicht über die Brisanz der Daten informiert und pflegen einen leichtsinnigen Umgang damit.
    - Schulen Sie Ihre Mitarbeiter in Datenschutzthemen.
- Datenschutzverstöße werden aus Gründen des Komforts begangen. Beispielsweise werden Kundendaten in einer unsicheren Umgebung zu Testzwecken vorgehalten.
    - Regeln Sie den Umgang mit datenschutzrelevanten Informationen und sanktionieren Sie Verstöße gegen Datenschutzvorschriften.
- Es werden zu viele Daten erhoben.
    - Hinterfragen Sie vor der Erhebung weiterer Daten die Notwendigkeit. Anyonymisieren oder pseudonymisieren Sie datenschutzrelevante Informationen – sofern möglich.
- Schutzpflichtige Daten werden zweckentfremdet.
    - Erhobene Daten dürfen nur für den angegebenen Zweck verwendet werden. Ein Berechtigungssystem kann die anderweitige Verwendung unterbinden und unzulässige Zugriffe protokollieren.
- Die Daten werden nicht ausreichend geschützt.
    - Mit der Erhebung personenbezogener Daten kommt die Verpflichtung einher, diese angemessen mit technischen Mitteln zu schützen. Die Wirksamkeit des Schutzes sollte regelmäßig mit geeigneten Methoden geprüft werden.

9. Systemfehler oder Systemausfälle

Beschreibung

Ein technischer Defekt von IT-Komponenten kann jederzeit auftreten. Nicht nur Hardware kann hierbei ein Problem darstellen, sondern auch die für den Betrieb notwendigen Ressourcen. Zum Beispiel kann eine Unterbrechung der Stromversorgung, eine gestörte Internetanbindung oder ein unzureichende Klimatisierung zu Systemausfällen führen.

Häufige Versäumnisse und wie man sie vermeidet

– Die Nichtverfügbarkeit eines Systems verursacht Probleme mit weiteren Systemen.

    - Identifizieren Sie die Abhängigkeiten der Systeme innerhalb ihres Unternehmensnetzwerks und dokumentieren Sie diese, um Lawineneffekte mithilfe weiterer Redundanzen verhindern zu können.

– Die Infrastruktur ist über Jahre hinweg gewachsen, eine Wartung ist aufgrund einer mangelnden Dokumentation sehr aufwändig.

    - Führen Sie eine Configuration Management Database (CMDB) ein. Dokumentieren Sie unter anderem die Komponenten, Standorte und Berechtigungen der unternehmenseigenen Hardware.

– Es gibt keinen eindeutigen Notfallplan für auftretende Systemfehler oder Systemausfälle.

    - Definieren Sie Prozesse und Verantwortlichkeiten für den Fall, dass Probleme auftreten. Je nach Kritikalität der möglicherweise ausfallenden Hardware, müssen Ersatzteile vorhanden oder zumindest deren Beschaffunswege und -zeiten bekannt sein. Die für die Behebung notwendigen Ressourcen sollten nicht durch einen Systemfehler oder -ausfall beeinflusst werden. Entkoppeln Sie diese oder sorgen Sie für ausreichende Redundanzen.

– Mitarbeiter melden Hardware- oder Softwareprobleme nicht, weil Ansprechpartner nicht bekannt sind oder Ihnen der Problemlösungsprozess zu aufwändig ist.

    - Ermöglichen Sie die Meldung und Weitergabe von Hinweisen. Sorgen Sie für eine frühzeitige Behandlung von bekannten Problemen.

Zusammenfassung

Die Grundlage einer effektiven und effizienten Cybersicherheit ist die regelmäßige Auseinandersetzung mit dem Thema. Führen Sie dazu z. B. einen „Quick Run“ mittels des KPMG Cyber Security Maturity Assessment (CSMA) durch.

https://atlas.kpmg.de/business-assessments/cyber-security-maturity-assessment.html

Führen Sie alternativ eine ausführlichere Reifegradbestimmung und Optimierungsberatung mittels KPMG „CyberSAFE“ durch. Experten aus den Bereichen Prävention, Detektion und Reaktion besprechen mit Ihnen den Status Quo Ihrer Cybersicherheit und geben maßgeschneiderte Empfehlungen für die Optimierung Ihrer Strukturen und Prozesse.

Kontakt

Michael Sauermann
Partner, Head of Forensic Technology Germany
T +49 30 2068-4624
msauermann@kpmg.com

www.kpmg.de