Cyberangriffe – Risiken, Prävention und Reaktion

von Dr. Marian Corbe, Theresa Grassl, Essen

Cyberkrieg: Ahnungslos ins Chaos?

Risiken

Durch die zunehmende Digitalisierung von Geschäftsprozessen und die damit einhergehende Abhängigkeit von Informationstechnologie, steigen auch die Risiken von Cyberangriffen für Unternehmen. Immer häufiger berichten Medien von Angriffen auf bekannte Unternehmen, mit oftmals schwerwiegenden Folgen. Die Schlussfolgerung, dass Cyberkriminelle nur ökonomische Schwergewichte anvisieren und KMUs keine lukrativen Ziele darstellen, wird oft als Argument gegen die Bereitstellung von Ressourcen für IT-Sicherheit verwendet. Dies ist jedoch ein Trugschluss! Unternehmen jeder Größenordnung und Branche sind lukrative Ziel für immer professioneller agierende Cyberkriminelle.

Wenn IT-Systeme plötzlich nicht mehr verfügbar sind, verursacht dies oft den Ausfall wichtiger Geschäftsprozesse im Tagesgeschäft, mit unmittelbaren finanziellen Auswirkungen, z.B. in der produzierenden Industrie oder im Handel. Besteht zudem der Verdacht, dass Geschäftsgeheimnisse oder personenbezogene Daten abgegriffen wurden, kann ein Cyberangriff auch gravierende Reputationsschäden und rechtliche Folgen nach sich ziehen. Insgesamt ergibt sich ein Spektrum folgender Schäden:

- Verlust des Zugriffs auf unternehmenseigene Informationen und IT-Systeme
- Betriebsunterbrechungen und Notbetrieb über mehrere Tage
- Diebstahl von sensiblen Unternehmensinformationen (Kundendaten, Geschäftsgeheimnissen, Patenten) oder von personenbezogenen Daten
- Imageschäden und Vertrauensverlust bei Kunden
- Wiederherstellungskosten für Bereinigung und/oder Neuanschaffung von IT-Systemen

Im schlimmsten Fall können diese Schäden zu einer wirtschaftlichen Schieflage bis zur Insolvenz der betroffenen Unternehmen führen.

Daher empfiehlt es sich, IT-Sicherheit nicht als unnötigen Kostenfaktor anzusehen – Prävention ist im Verhältnis zu einem Schaden die günstigere Alternative!

Prävention

Um den Gefahren eines Cyberangriffs entgegenzuwirken, sollten Sie das Thema IT-Sicherheit als ganzheitliche Aufgabe verstehen, der Sie mit gezielten organisatorischen, technischen, personellen und infrastrukturellen Maßnahmen begegnen können.

Ein erster Ansatz sollte immer eine Analyse der wertschöpfenden Geschäftsprozesse und der damit verbundenen IT-Systeme und Datenflüsse sein, damit Sie einen Ausgangspunkt für Ihre individuelle Risikoanalyse haben.

Im Folgenden stellen wir (verkürzt) einige der klassischen größten Sicherheitsrisiken dar, die mit geringem Aufwand reduziert werden können.

Fehlende Sicherheitsupdates. Sicherheitslücken in IT-Systemen stellen technische Schwachstellen dar, die Schadsoftware ausnutzt. Oft werden spezifische Sicherheitsupdates von Herstellern bereitgestellt, um entdeckte Lücken zu schließen. Daher ist es unerlässliche, IT-Systeme regelmäßig mit den neuesten Updates zu aktualisieren.

Unregelmäßige Datensicherungen. Ransomware-Angriffe zielen darauf ab, Daten zu verschlüsseln und somit unzugänglich zu machen. In diesem Szenario sind Datensicherungen die Rettung eines Unternehmens. Daher sollten in Zeitintervallen, die einen tolerierbaren Datenverlust widerspiegeln, vollständige Datensicherungen der Systeme durchgeführt werden. Wichtig ist, dass die Datensicherungen so aufbewahrt werden, dass sie nicht ebenfalls kompromittiert werden können.

Unsichere Passwörter. Ursache für die meisten Sicherheitsvorfälle sind schwache Passwörter. Diese können von Angreifern leicht ausgespäht oder gehackt werden. Um dem vorzubeugen, sollten Mindestanforderungen an Passwörter festgelegt werden. Zudem ist es ratsam, Mitarbeitende anzuweisen, keine Haftnotizen mit dem Passwort an den Bildschirm des PCs zu hängen.

Faktor Mensch. Gängige Angriffsarten wie Phishing zielen auf den Menschen als Schwachstelle ab. Bereits durch einen Klick auf einen Mailanhang oder einen Link kann das IT-System

eines Unternehmens lahmgelegt werden. Die Sensibilisierung der Mitarbeitenden zu Gefahren und dem richtigen Umgang mit bereitgestellter IT ist daher unerlässlich und ein wesentliches Element der IT-Sicherheit – technische Maßnahmen alleine sind nicht ausreichend!

Nutzung privater Endgeräte. Es werden oft private Endgeräte im betrieblichen Kontext genutzt. Durch die unzureichende Absicherung dieser Geräte und fehlende Kontrolle des Arbeitgebers, ergeben sich Sicherheitsrisiken, auch in Verbindung mit dem Datenschutz. Daher muss das Ob und das Wie der Nutzung privater Endgeräte durch Mitarbeitende unbedingt geregelt werden.

Mobiles Arbeiten. Mobiles Arbeiten im Homeoffice oder auf Dienstreisen ist ein Risiko für die IT-Sicherheit. Netze und Zugänge liegen außerhalb der Kontrolle des Unternehmens, das Risikobewusstsein sinkt im vertrauten Umfeld. Werden Daten lokal gespeichert, so werden sie nicht in der Datensicherung erfasst. Daher sollten klare Regelungen für das mobile Arbeiten geschaffen werden. Technische Maßnahmen, wie die Absicherung des Zugriffs auf das Firmennetz mit VPN, ergänzen diese.

Reaktion

Das Risiko eines Cyberangriffs lässt sich reduzieren aber nicht ausschließen. Was also tun, wenn ein Unternehmen doch Ziel eines Cyberangriffs wird? Mit dieser Fragestellung befasst sich das IT-Notfallmanagement, im Rahmen dessen man sich im Vorfeld mit dem Ernstfall auseinandersetzt und einen Handlungsleitfaden entwirft. Dies dient gleichermaßen der Minderung der Auswirkungen und der Bewältigung des Vorfalls. Die Identifikation von Handlungsoptionen, Stakeholdern und Kommunikationswegen ermöglicht eine schnelle Reaktion auf den Vorfall, während die Geschäftstätigkeiten im Notbetrieb aufrechterhalten werden.

Durch die Identifikation kritischer Geschäftsprozesse, eine klare Zuweisung von Rollen, Melde- und Entscheidungsprozessen sowie von Kommunikationswegen, können gezielt Notfallpläne zum Umgang mit Cyberangriffen erstellt werden.
Die Anwendung dieser ermöglicht einen strukturieren Umgang mit IT-Notfällen, wodurch sich die finanziellen Auswirkungen verringern und der Komplettausfall des Geschäftsbetriebs sowie tiefgehender Image-Verlust vermeiden lassen.

10 Prüffragen zum Stand der IT-Sicherheit in Ihrem Unternehmen

Nehmen Sie sich 30 Minuten Zeit für die Umsetzungsaufgabe und stellen sich die 10 folgenden Prüffragen zum Stand der IT-Sicherheit in Ihrem Unternehmen.

1. Welche Auswirkung hat ein möglicher Ausfall Ihrer IT-Systeme?
2. Sind Sie auf einen Ausfall Ihrer IT-Systeme vorbereitet?
3. Schulen Sie Ihr Personal zum Umgang mit IT und Themen der IT-Sicherheit?
4. Haben Sie Schutzmaßnahmen für den Umgang mit sensiblen Daten etabliert?
5. Haben Sie Regelungen für die Themen Passwortsicherheit, Homeoffice, die Nutzung privater Endgeräte und die Internetnutzung in Ihrem Unternehmen eingeführt?
6. Sind Ihre IT-Systeme technisch abgesichert, z.B. durch Firewalls, Virenschutz, Webfilter und regelmäßige Sicherheitsupdates?
7. Erstellen Sie regelmäßig ein Backup Ihrer Daten?
8. Erhalten alle Mitarbeitenden eigene Nutzerkonten mit eindeutig zuordenbarer Zugangskennung und individuellen Passwörtern?
9. Existiert ein Notfallkonzept für den Ernstfall, das allen Mitarbeitenden bekannt ist?
10. Verfügen Sie über Fachpersonal oder externe Dienstleister, die Sie im Ernstfall unterstützen können?

Fazit und Chancen

Ein Cyberangriff kann jedes Unternehmen treffen. Das Ergreifen organisatorischer, technischer, personeller und infrastruktureller Präventivmaßnahmen dient der Reduktion dieses Risikos und ist bereits mit geringen Mitteln möglich. Eine vorausschauende Planung und Vorbereitung auf den Ernstfall ergänzen diese Maßnahmen und reduzieren hohe betriebswirtschaftliche und rechtliche Risiken. Die individuellen Ergebnisse der genannten Prüffragen bieten einen Einstiegspunkt.
Im Rahmen einer Sanierung gelten die Risiken natürlich auch für Insolvenzverwalter selbst, sie bieten jedoch auch Chancen. Wird die IT-Sicherheit als begleitende und ganzheitliche Aufgabe in einem Sanierungs- oder Restrukturierungsprojekt bedacht, können sich Synergien für die Neuaufstellung ergeben – insbesondere bei digitalen Geschäftsmodellen.

RST
Wirtschaftsprüfung · Steuerberatung
Rechtsberatung · Unternehmensberatung

Dr. Marian Corbe ist seit 2020 Geschäftsführender Gesellschafter der RST Informationssicherheit GmbH in Essen. Seine Tätigkeitsschwerpunkte liegen in der Implementierung von Managementsystemen der Informationssicherheit und der Umsetzung des IT-Sicherheitsgesetzes bei Betreibern Kritischer Infrastrukturen.

Theresa Grassl ist seit 2020 als Beraterin bei der RST Informationssicherheit GmbH tätig. Ihre Themenschwerpunkte sind die organisatorische Umsetzung der Informationssicherheit und des Notfallmanagements.