Und täglich grüßt der Cyberschaden …

Verwundbare IT: Szenarien und Absicherung

Sandra Dammalacks

Hackerangriffe, Malware und Datendiebstähle sind längst Alltag geworden. Gefeit davor sind weder Privatpersonen noch staatliche Institutionen und Unternehmen. Attacken wie in der jüngsten Vergangenheit durch WannaCry oder vergleichbare Ransomware zeigen: Die digitalisierte Welt macht Unternehmen verwundbarer denn je.

Durch Schadsoftware werden Computersysteme infiziert und Daten verschlüsselt. Für die (vermeintliche) Entsperrung der Daten verlangen die Täter dann meist ein Lösegeld. Schätzungen zufolge wird auf diese Weise jährlich rund 1 Mrd. USD erpresst. Allein das Virus WannaCry hat Daten von mehr als 220.000 Computern verschlüsselt. Als Folge kam es in den betroffenen Unternehmen u. a. zu massiven Betriebsunterbrechungen.

Zwar hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) wiederholt davon abgeraten, auf die Lösegeldforderungen der Hacker einzugehen, doch viele Opfer, die auf wichtige und sensible Daten nicht mehr zugreifen können, halten sich nicht an den Rat in der Hoffnung, mit der Zahlung weitere verheerende Folgen für das Unternehmen abwenden zu können.

Das Ergebnis ist, dass sich mittlerweile eine wahre Industrie für Ransomware entwickelt hat, die an diesen Szenarien kräftig verdient. Dass sich die für die Täter äußerst lukrativen Attacken wiederholen, ist daher vorprogrammiert. Einmal mehr hat das der jüngste Angriff gezeigt, der u. a. Großkonzerne wie Maersk und Beiersdorf getroffen hat. Studien legen den Schluss nahe, dass derartige Attacken jährlich um bis zu 50 % zunehmen werden.

Unternehmen auf der ganzen Welt müssen sich daher heute intensive Gedanken machen, wie sie ihre IT bestmöglich gegen Cyberattacken schützen können.

Risikoszenarien unterschiedlich

Je nach Branche unterscheiden sich die Risiken im Cyberbereich sehr stark. Das Risikoportfolio hängt von den betrieblichen Abläufen und den verwendeten Technologien im jeweiligen Unternehmen ab. Das Verständnis für die individuelle Risikolage und die Gefährdungspotenziale ist die Voraussetzung dafür, die möglichen Auswirkungen von Schäden erfassen zu können und dementsprechend Verhinderungsmaßnahmen zu evaluieren.

Nicht nur die jeweiligen Netzwerkstrukturen und Datenbestände müssen in eine genaue Betrachtung mit einfließen, sondern auch die gespeicherten und verarbeiteten Daten. Zudem sind die Rahmenbedingungen für die IT-Sicherheit im Unternehmen zu bewerten. Hier stehen beispielsweise Fragen im Vordergrund wie: Wie sieht es mit dem Brandschutz aus? Ist eine Notstromversorgung verfügbar? Inwieweit sind Server und Rechenzentren vor Angriffen geschützt? Was wird gegen etwaige Sicherheitsrisiken bei outgesourcten IT-Leistungen getan? … Bereits bestehende Sicherheitsrichtlinien und -verfahren sowie Notfall- und Krisenpläne, soweit vorhanden, sind ebenfalls Gegenstand der Risikoanalyse.

Am Ende des Tages hat man eine detaillierte Risk Landscape der eigenen Cyberrisiken zur Hand. Dass man das entsprechende Know-how hierfür nicht unbedingt im Haus hat, ist kein Beinbruch. Glücklicherweise kann man heutzutage ja auf externe Expertise zurückgreifen.

Gesetzliche Anforderungen verschärft

Mit Inkrafttreten des IT-Sicherheitsgesetzes für Deutschland (2015) sowie der Europäischen Datenschutz-Grundverordnung (EU-DS-GVO, ab 2018) müssen sich Unternehmen im Zusammenhang mit Cybersicherheit und Datenschutz mit verschärften Auflagen auseinandersetzen.

Prüfnachweise für KRITIS

Nach dem IT-Sicherheitsgesetz müssen deutsche Unternehmen bereits zum 3. Mai 2018 erste Prüfungsnachweise vorlegen, um zu dokumentieren, dass sie bestimmte Sicherheitsvorschriften nach dem Stand der Technik vorgenommen haben. Betroffen von der Prüfpflicht durch das BSI sind die so genannten KRITIS (Betreiber Kritischer Infrastrukturen).

Dazu zählen Unternehmen aus den Sektoren Energie, Telekommunikation, Informationstechnik, Transport oder Verkehr wie auch Unternehmen aus den Bereichen Wasser, Ernährung sowie Finanz- und Versicherungswesen.

Verschärfung durch EU-Richtlinie
Während sich das IT-Sicherheitsgesetz mit Kritischen Infrastrukturen befasst, ist die Europäische Datenschutz-Grundverordnung darauf ausgerichtet, europaweit eine einheitliche und verbindliche Regelung für Datensicherheit zu schaffen. Alle Unternehmen, die mit Daten von EU-Bürgern arbeiten, sind betroffen – auch wenn sie ihren Sitz außerhalb der EU haben. Bis zum Inkrafttreten am 25. Mai 2018 müssen Firmen dafür Sorge tragen, dass europäische Privatpersonen mehr Kontrolle darüber enthalten, wie und zu welchem Zweck ihre Daten verarbeitet werden.

Der bereits existierende Bußgeldkatalog für „Datensünder“ wird sich mit Inkrafttreten der EU-DSGVO nochmals verschärfen. Bei Verstößen gegen IT-Sicherheitspflichten oder gegen die Informationspflicht den zuständigen Behörden bzw. den Betroffenen gegenüber belaufen sich die neuen Bußgelder für Unternehmen auf bis zu 10.000.000 Euro bzw. auf 2 % ihres gesamten Vorjahresumsatzes weltweit – je nachdem, welcher der beiden Beträge höher ist. Zudem können weitere Anordnungen der Aufsichtsbehörden erfolgen.

Cyberversicherungen eine Lösung?
Bedingt durch die Vielzahl der Cybervorfälle und durch die beinahe tagtäglichen Medienberichte, hat sich die Cyberversicherung vom einstigen Nischenprodukt innerhalb weniger Jahre ins Bewusstsein der Unternehmer eingebrannt. Nichtsdestoweniger ist zu betonen: Diese Deckung ist kein Allheilmittel gegen Cyberattacken. Vielmehr setzen die Versicherer vor Abschluss des Versicherungsvertrags eine bereits gut funktionierende ITLandschaft im Unternehmen voraus und prüfen dies – besonders bei komplexen Risiken – in Form von Risikodialogen auch sehr genau ab. Insofern ist die Cyberversicherung lediglich das berühmte i-Tüpfelchen auf einem komplexen IT-Sicherungskonzept, das hilft, die Kosten für den Fall eines Schadeneintritts kalkulierbar zu machen.

Die Cyberversicherung ist ein Kombinationsprodukt, das sich aus verschiedenen Bausteinen zusammensetzt.
Die Versicherungsbedingungen unterscheiden sich bei den einzelnen Anbietern erheblich, stellen jedoch in der Regel alle auf zwei Grundtypen von Versicherungsfällen ab: den Cybervorfall und die Datenschutzrechtsverletzung.

Wenn von einer Datenschutzrechtsverletzung die Rede ist, geht es immer um einen nicht ordnungsgemäßen Umgang mit Daten, die unter die Datenschutzbestimmungen fallen; das sind zumeist personenbezogene Daten. Spricht man indes von einem Cybervorfall, ist immer ein unberechtigter Zugriff auf das IT-System gemeint. Dies kann der bösartige, zielgerichtete Hack eines Saboteurs sein oder auch das unbewusste Öffnen eines mit Schadsoftware kontaminierten Mailanhangs. Versicherbar sind sowohl die Folgen eines konkreten Hackerangriffs, der sich in einen Erpressungsfall auswachsen kann, als auch die Folgen einer Fehlbedienung durch eigene Mitarbeiter.

Die durch diese Schadenszenarien entstehenden (Zusatz-)Kosten sind in der Cyberdeckung entschädigungspflichtig.

Unter den Versicherungsschutz fallen

> Ertragsausfall
> Ausfall der Telekommunikation/ Website
> Bedienfehler
> DoS-Attacke
> Hackerangriff
> Manipulation durch eigene Mitarbeiter
> Ausfall von IT-Dienstleistungen
> Sachverständigenkosten
> Datenwiederherstellung
> Rufschädigung/Krisenmanagement
> Datenschutzverletzung
> Internetbetrug
> Erpressung
> Cyberhaftpflicht

Neben den Schadenersatzleistungen für Drittschäden und für entgangenen Gewinn gehört die Erstattung von Forensikkosten und Assistenzleistungen im Krisenfall (meist via Hotline des Versicherers) zu den wichtigsten Leistungsbestandteilen der Cyberversicherung.

Einige Versicherer bieten als inkludierte Zusatzleistung sogar die Erarbeitung neuer bzw. die Überprüfung bestehender Krisenpläne an. Dabei bedienen sie sich oft externer Dienstleister, mit denen sie vorteilhafte Kooperationskonditionen vereinbart haben, was durchaus zu einer Win-Win-Situation für alle Seiten führen kann. Letztendlich muss das Management des jeweiligen Unternehmens entscheiden, ob es lieber ein All-in-one-Produkt kauft oder unabhängig von der Versicherungs-

leistung einen eigenen Dienstleister beauftragt.

Unterm Strich empfiehlt sich vor Abschluss einer Cyberversicherung aufgrund der sehr unterschiedlichen Bedingungen und Leistungsangebote am Markt eine individuelle und maßgeschneiderte Beratung.

Nur mit professioneller Analyse des Risikoportfolios kann sichergestellt werden, dass das Versichererprodukt bzw. das Maklerwording tatsächlich zum eigenen Unternehmensrisiko passt.

Gerne stehen Ihnen die Experten im Center of Competence für eine ausführliche Beratung und für das Einholen von passenden Angeboten zur Verfügung.

Fragen Sie Ihren Kundenbetreuer danach.