Gefahren erkennen und verstehen
Cyberangriffe

Organisatorische Maßnahmen

Durch die steigende Anzahl an Cyberangriffen müssen sich immer mehr Unternehmen auf finanzielle Verluste und Schädigungen ihrer geschäftlichen Reputation einstellen, sofern sie sich nicht auf ihre Verteidigung vorbereitet haben und bei Angriffen umgehend reagieren können.

Gefahrenbereiche:

- Bauliche Ausführung
- Ausstattung
- Brandschutz
- **Organisatorische Maßnahmen**
- Elementarrisiken
- Prozesse und ihre Gefahrenpotenziale

Dies ist eine Broschüre aus der Reihe „Gefahren erkennen und verstehen", die Ihnen helfen soll, übliche Gefahrenpotenziale in Ihrem Betrieb zu identifizieren und Verbesserungen durchzuführen. Wenn Sie weitere Informationen zur Gefahrenerkennung innerhalb Ihres Unternehmens erhalten möchten, wenden Sie sich bitte an FM Global.

Gefahren erkennen

Die Bedrohung durch Cyberrisiken ist allgegenwärtig. Die Frage ist nicht mehr, ob, sondern wann Ihr Unternehmen Opfer eines Cyberangriffs wird. Die Anzahl der jährlich gemeldeten Cyberangriffe wächst exponentiell und eine Verlangsamung dieser Entwicklung ist nicht abzusehen. Medienberichte über hochprofessionelle Cyberkriminalität, die hohe Kosten verursacht, wecken zurzeit das Bewusstsein für Cyberrisiken als Herausforderung für das gesamte Unternehmen, nicht nur für die IT-Abteilung. Da solche Angriffe nicht nur von außen, sondern auch von innen drohen, muss man sich sowohl um die internen als auch um die externen Schwachstellen kümmern.

Einige Szenarien für Cyberangriffe beinhalten Datenschutzverletzungen von Kundendaten durch Unbefugte, die sich mit den Informationen aus diesen Datensätzen Vorteile verschaffen. Andere Szenarien sind durch übermäßigen Datenverkehr bewusst hervorgerufene Serverausfälle, die ein Netzwerk überlasten und den Zugriff auf Webseiten und Mobilanwendungen vollständig unmöglich machen. Oder ein Hacker nutzt Schwachstellen im Netzwerk, um böswillig Umspannwerke anzugreifen und Stromausfälle bei Tausenden, wenn nicht Millionen Kunden zu verursachen.

Der Verlust von wichtigem geistigen Eigentum und personenbezogenen Datenressourcen ist jenes Risiko, das am häufigsten mit Cyberangriffen assoziiert wird. Aber auch Sachschäden stellen eine sehr reale Gefahr dar. Hacker können beispielsweise das Überdrehen einer Turbine und damit erheblichen Schaden an empfindlichen, hochwertigen Maschinen verursachen. Es gibt noch viele weitere Risiken im Zusammenhang mit Cyberangriffen, denen begegnet werden muss, darunter Betriebsunterbrechungen und nachfolgende Verluste von Marktanteilen, hohe Bußgelder, restriktivere Vorschriften und – vielleicht der größte Schaden – langfristige, negative Auswirkungen auf Ihre geschäftliche Reputation.

Was können Sie tun?

Sofortmaßnahmen:

- Stellen Sie fest, welche Datensicherheitsrichtlinie für Ihre Branche anwendbar ist, und erstellen Sie Ihre Rahmenstruktur für die Cybersicherheit auf Grundlage dieser Vorgaben. Bei fehlenden klaren Anweisungen von Seiten ihrer Branche empfehlen wir Unternehmen, das Cybersicherheitsregelwerk *Framework for Improving Critical Infrastructure Cybersecurity* des US-amerikanischen National Institute of Standards and Technology (NIST) zu übernehmen.
- Ermitteln und klassifizieren Sie Daten anhand ihrer betriebswirtschaftlichen Bedeutung sowie ihrer Sensibilität und Vertraulichkeit.
- Ermitteln Sie kritische Ressourcen und die physischen/logischen Netzwerk-Zugangspunkte in Ihrer Einrichtung und finden Sie heraus, wie der Zugriff darauf kontrolliert wird. Priorisieren Sie Ihre Maßnahmen zur Verbesserung der Kontrolle über den physischen Zugriff/Fernzugriff auf diese ermittelten Ressourcen und Netzwerk-Zugangspunkte. Empfehlungen hierzu erhalten Sie auf Anfrage bei FM Global im FM Global Datenblatt zur Schadenminimierung 9-1, *Supervision of Property*.

Mittelfristige Maßnahmen:

- Erarbeiten und pflegen Sie einen schriftlichen Notfallplan, damit Ihre Mitarbeiter bei Cyberangriffen angemessen reagieren können. Dieser Plan darf nicht nur ein einzelnes Dokument darstellen, sondern sollte Teil eines vollständigen Risikomanagementprogramms sein.
- Testen Sie die Anwendung des Notfallplans. Übungen mit simulierten Angriffen sind eine sehr wirkungsvolle Methode, um die Angemessenheit eines Plans und die Zeitrahmen für die Datenwiederherstellung zu testen.

Gefahren verstehen

Cyberangriffe können viele Formen annehmen. Im Wesentlichen lassen sie sich aber in zwei Kategorien gliedern: Virus-/Malware-Angriffe und Denial-of-Service-Angriffe.

Malware-Angriffe bestehen normalerweise aus der Einführung eines nicht autorisierten Computer-Codes in das Host-System, sei es über einen verbreiteten Computervirus oder über einen gezielten Hacker-Angriff. Solche Angriffe können auch zu Sachschäden – also nicht nur zu Datenschäden – und einer damit verbundenen Betriebsunterbrechung führen. Eine weitere, neu aufkommende Art von Malware ist die Ransomware. Dabei handelt es sich um eine bösartige Software, die den Zugriff auf das infizierte Computersystem verhindert. Bei einigen Formen der Ransomware werden Dateien systematisch verschlüsselt. Erst nach Zahlung eines „Lösegeldes“ (Ransom) wird die Entschlüsselung ermöglicht.

Denial-of-Service-Angriffe (DoS) erfolgen gewöhnlich durch gezielte Überlastung sendender oder empfangender Systeme mit Anforderungen, unter deren Masse das angegriffene System zusammenbricht.

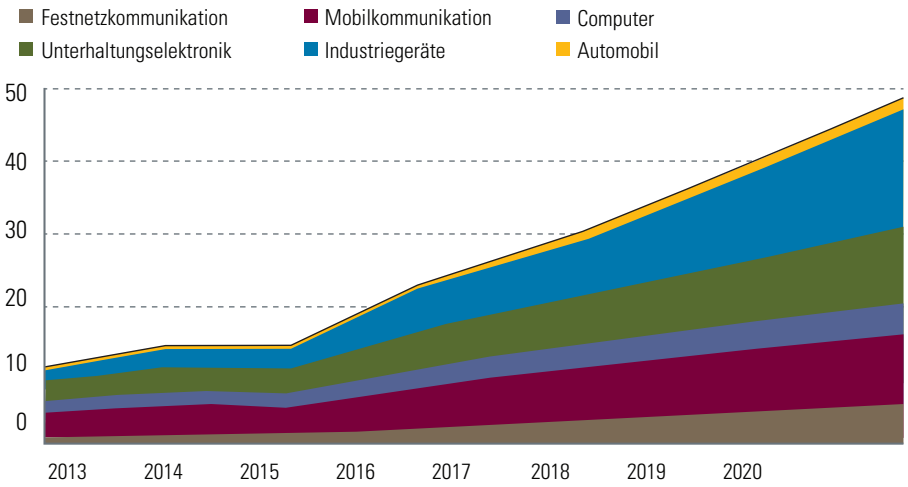
Für alle Formen von Cyberangriffen ist zunächst ein Netzwerkzugriff erforderlich. Hacker verschaffen sich diesen Zugriff entweder physisch (z. B. durch Einstecken eines Flash-Laufwerks in einen Computer-Port) oder virtuell (z. B. über eine Internetverbindung).

Schadenbilanz

Laut der Umfrage „Global State of Information Security® Survey“, die von PricewaterhouseCoopers durchgeführt wurde, hat sich die Anzahl der Cyberangriffe 2015 um 38 Prozent gegenüber 2014 erhöht. Zudem überschreiten laut einer Studie des Ponemon Institute aus dem Jahr 2015 die durchschnittlichen jährlichen Kosten für Cyberkriminalität weltweit mittlerweile 7,7 Millionen USD. Außerdem berichtet Cisco Systems, Inc., dass sich bis 2020 die Anzahl der internetfähigen Geräte weltweit um über 200 Prozent erhöhen wird, was die Cyberrisiken noch deutlich steigert.

Die 50-Milliarden-Frage

Weltweite Anzahl von Geräten mit Internetverbindung; Prognose



Quelle: Cisco

*Einschließlich Militär und Luftfahrt

Ein Schadenfall zur Veranschaulichung: Bedrohung durch internen Mitarbeiter

Ein Mitarbeiter manipulierte ein Programm zum Benchmarken der Spezifikationen für ein sehr wertvolles firmeneigenes Computersystem. Das Unternehmen wandte sehr viel Zeit auf, um die Ursache für die dadurch entstandenen Probleme zu ergründen. Aufgrund der Idee, die Probleme könnten vielleicht aus dem Raum stammen, in dem die Tests durchgeführt wurden, wurde das gesamte Projekt an einen anderen Standort verlegt. Später wurde dieser Mitarbeiter dabei ertappt, wie er auf den Computer eines Kollegen zugriff. Von der Leitung zur Rede gestellt, gestand er, die Probleme verursacht zu haben. Bis dahin hatte das Unternehmen jedoch bereits einige Millionen Dollar und Unmengen von Zeit vergeudet.

Aber...

... wenn Cyberangriffe doch unvermeidlich sind? Warum überlassen wir sie nicht einfach unserer Versicherungsgesellschaft und den Strafverfolgungsbehörden?
Angesichts der Art dieser Verbrechen und der Komplikationen, die mit der Durchsetzung der Gesetze verbunden sind, werden Hacker kaum vor Gericht zur Rechenschaft gezogen. FM Global geht grundsätzlich davon aus, dass die Mehrheit aller Verluste, auch durch Cyberangriffe, vermeidbar ist, und dass es leichter ist, Schaden zu vermeiden, als sich davon zu erholen. Zusammen mit unseren Kunden versuchen wir, ihre Risiken im Zusammenhang mit IT-Systemen zu verringern und Schäden an den Systemen mit bewährten Prinzipien zur Verbesserung der Risikoqualität zu mindern.

... wenn unser Unternehmen doch gar nichts zu bieten hat, woran ein Hacker interessiert sein könnte? Sind Zeit und Geld nicht andernorts besser investiert?
Es ist richtig, dass in einigen Branchen aufgrund der Art des Geschäfts und der gespeicherten Daten Cyberangriffe wahrscheinlicher sind als in anderen Branchen. Aber nur weil in Ihrer Branche das Risiko geringer ist, sind Sie noch lange nicht immun gegen künftige Cyberangriffe. Da das Internet der Dinge weiter anwächst und die Anzahl der Geräte mit Internetverbindung sich erhöht, steigt auch die Wahrscheinlichkeit von Verlusten in Verbindung mit Cyberangriffen. Die Motive der Hacker sind schwer zu ergründen, und einige tun es aus dem einfachen Grund, dass sie es können. Leider werden sich aber mit ihren zunehmenden Fähigkeiten und Ressourcen auch ihre Ziele ausdehnen.

Definitionen

Denial-of-Service-Angriffe (DoS): Angriffe, die speziell darauf ausgerichtet sind, die normalen Funktionen eines Systems zu unterbinden und den Zugriff auf das System durch autorisierte Benutzer zu verhindern. Hacker können Denial-of-Service-Angriffe verursachen, indem sie die Server des Systems überlasten und den legitimen Zugriff auf den Service verhindern.

Industrielles Steuerungssystem (ICS): Ein allgemeiner Ausdruck, der mehrere Arten von Steuerungssystemen beschreibt, darunter SCADA-Systeme (Supervisory Control and Data Acquisition – „Überwachung, Steuerung und Datenerfassung“), dezentrale Steuerungssysteme (DCS) und andere Steuerungssystem-Konfigurationen wie z. B. aufgesetzte speicherprogrammierbare Steuerungen (SPS), die in Bereichen der industriellen Steuerung und in kritischen Infrastrukturen häufig anzutreffen sind. Ein ICS besteht aus Kombinationen von Steuer- und Sensorbauteilen (z.B. elektronisch, mechanisch, hydraulisch oder pneumatisch), die interagieren, um bestimmte Zielvorgaben zu erreichen (z.B. in der Herstellung, im Material- oder Energiefluss).

Internet der Dinge („Internet of Things“, IoT): Netzwerk physischer Objekte, z. B. Geräte, Fahrzeuge, Gebäude, in das Elektronik, Software, Sensoren und Netzwerkverbindungen integriert sind, mit denen diese Objekte Daten erfassen und austauschen können.

Weitere Informationen

Fragen Sie unser Kundenbetreuungsteam nach folgendem Informationsmaterial:

- FM Global Datenblatt zur Schadenminimierung 9-1, *Supervision of Property*
- 2016 Cyber Coverage Enhancements Sell Sheet
- 2016 Cyber Coverage Enhancements Video

Ransomware: Software, die die Festplatte des infizierten Computers verschlüsselt und dem Hacker die Möglichkeit gibt, vom Eigner des Computers ein Lösegeld zu verlangen, woraufhin der Eigner die Entschlüsselungssoftware erhält, mit der er die Daten wieder nutzbar machen kann.

Schadprogramm („Malware“): Bösartige Software wie Viren, Trojaner, Spyware (Spionageprogramme) sowie bösartiger aktiver Inhalt.

Verschlüsselung: Umwandlung von Daten in eine unlesbare Form, die nur mithilfe eines bestimmten Schlüssels aufgelöst werden kann.

Virus: Ein Computerprogramm, das sich selbst an Festplatten oder Dateien anhängt und sich mehrfach repliziert, meist ohne Wissen oder Erlaubnis des Benutzers. Einige Viren bilden Symptome aus, aber besonders schädliche Viren beschädigen die Dateien und Computersysteme unbemerkt. Viren verfügen über eine Reihe von Methoden, um Computer zu infizieren. Einige warten, bis die infizierte Datei ausgeführt wird, während andere die Dateien infizieren, wann immer auf dem Computer Dateien geöffnet, geändert oder erstellt werden.

Das sollte Ihnen nicht passieren...

Ein Stahlwerk wurde Opfer eines Angriffs auf sein ICS. Die Hacker manipulierten und unterbrachen Steuerungssysteme in einem solchen Ausmaß, dass ein Hochofen nicht richtig abgeschaltet werden konnte. So entstand erheblicher Schaden.

Bestellung von Informationsmaterial

Weitere Exemplare aus der Reihe *Gefahren erkennen und verstehen* können über Ihren FM Global Ingenieur oder Ihr FM Global Kundenbetreuungsteam bezogen werden.

Weitere FM Global-Publikationen und Schulungsmaterialien sind im FM Global Resource Catalog zu finden und können unter der folgenden Internetadresse online bestellt bzw. heruntergeladen werden: www.fmglobalcatalog.com. Falls Sie eine persönliche Beratung wünschen, zögern Sie nicht, sich mit uns in Verbindung zu setzen:

- Gebührenfrei: +(1) 877 364 6726 (Kanada und USA)
- Telefon: +1 (1)401 477 7744
- Fax: +1 (1)401 477 7010
- E-Mail: germ.custserv@fmglobal.com