Widerstandsfähig bleiben

Damit in jeder Bedrohungslage der Betrieb weiterläuft

Elmar Geese

Cyberattacken haben sich zum größten Geschäftsrisiko entwickelt, das sich mit klassischen Sicherheitsmethoden nicht ausreichend mindern lässt. Widerstandsfähig werden Betreiber kritischer Infrastrukturen (Kritis) wie Energieversorger und Telekommunikationsanbieter mit einem durchdachten Cyberresilienzkonzept. Wie sich Unternehmen dadurch immer besser absichern können, geht aus einer Studie von Greenbone Networks und Frost & Sullivan hervor.

Elmar Geese ist COO der Greenbone Networks in Osnabrück

In Deutschland kostet ein verlorener oder gestohlener Datensatz ein Unternehmen im Schnitt 172 €. Ein sicherheitsrelevanter Vorfall betrifft im minderschweren Fall fast 27.000 Datensätze, was pro Datenpanne den finanziellen Schaden auf 4,25 Mio. € im Mittel hochschraubt. Diese Rechnung macht die IBM-Studie „2019 Cost of a Data Breach" auf, die das Ponemon Institut durchgeführt hat. Nach dessen Analyse verursachen Cyberattacken die Hälfte der Datenverluste in Unternehmen. Die Bedrohungslage verschärft sich zusehends, was sich auch im „Allianz Risk Barometer 2020" widerspiegelt. Diese Umfrage führt zum ersten Mal Cybervorfälle als das weltweit wichtigste Geschäftsrisiko auf – vor der Betriebsunterbrechung, die lange Jahre das Ranking anführte.

Eine solche Attacke kann jede Firma treffen. Überraschend ist, dass die Angriffsziele meistens durchaus bekannt sind. Da viele Unternehmen jedoch noch auf ein professionelles Schwachstellenmanagement verzichten, das die Vielzahl der möglichen Angriffspunkte minimieren könnte, haben Kriminelle oft leichtes Spiel.

Beim Verhindern von Cybervorfällen gibt es für viele der Entscheider, die am „Cyber Resilience Report" von Frost & Sullivan und Greenbone teilnahmen, noch viel Luft nach oben. Insgesamt befragte die Studie 370 Organisationen in den USA, Großbritannien, Frankreich, Japan und Deutschland. Ein zentrales Ergebnis: Nur jedes dritte Unternehmen kann als Organisation mit hoher Cyberresilienz eingestuft werden. Finanz- und TK-Unternehmen sind cyberwiderstandsfähiger, Unternehmen im Transportsektor hingegen am wenigsten resilient.

Wie diese Situation branchenübergreifend verbessert werden kann, ergründet der Report ebenfalls. Er geht auch der Frage nach, was die Schlüsselfähigkeiten sind, die Unternehmen mittel- bis hochresilient machen – auch im Energie- und TK-Sektor?

Grundgedanke der Cyberresilienz

Digitale Resilienz bedeutet, handlungsfähig zu bleiben – vor dem Hintergrund, dass es sehr schwierig ist, mögliche Vorfälle vollkommen auszuschließen. Das Ziel: Ein Unternehmen soll so widerstandsfähig sein, dass es trotz eines Cybervorfalls seine Geschäftsergebnisse wie geplant erreicht. Resilienz beschränkt sich nicht darauf, das Risiko einer Cyberattacke zu minimieren. Der geschäftskritische Betrieb läuft idealerweise in jeder Situation und bei allen Bedrohungslagen weiter. Dieses Konzept setzt auf ganzheitliches Denken sowie agiles und gezieltes Handeln, falls es zu einem Cybervorfall kommt. Grundsätzlich sichert Cyberresilienz die digitalen Geschäftsprozesse ab, die innerhalb einer Organisation zur Wertschöpfung beitragen.

In der EU soll die NIS-Richtlinie (Directive on Security of Network and Information Systems) für ein hohes Resilienzniveau der Organisationen sorgen, die kritische Infrastrukturen betreiben. Aufgrund der Wichtigkeit dieser Unternehmen für eine funktionierende moderne Gesellschaft hat sich die Studie von Frost & Sullivan und Greenbone auf Organisationen in den Sektoren Energie, Finanzen, Gesundheit, TK, Transport und Wasser konzentriert. Zu den erwähnten kritischen Geschäftsprozessen kommt in diesen Kritis-Bereichen hinzu, dass ein möglicher Vorfall auch Auswirkungen auf die Versorgungslage haben kann.

Womit Energieversorger und TK-Anbieter kämpfen

Energieversorger müssen sowohl die Unternehmens-IT als auch Operatio-

nal Technology (OT) berücksichtigen, wenn sie hochresilient werden wollen. Mit jedem vernetzten Gerät, etwa für Smart Grids und Smart Meter, vergrößert sich auch die Angriffsfläche, die Cyberkriminelle nutzen könnten. Insgesamt steht die Energiewirtschaft vor einem komplexen, heterogenen Spektrum an Systemen, Geräten und Applikationen aus verschiedenen Generationen. Die Kombination aus Legacy-Systemen und brandneuen Geräten sorgt oft für Sicherheitslücken und Unzulänglichkeiten. Governance- und Regulierungsrichtlinien fordern zudem oft zu widersprüchlichen Handlungen auf. Wenn die IT-Verantwortlichen diese Sachlage ignorieren, wird unweigerlich jede IT-Sicherheitsarchitektur ineffizient und angreifbar.

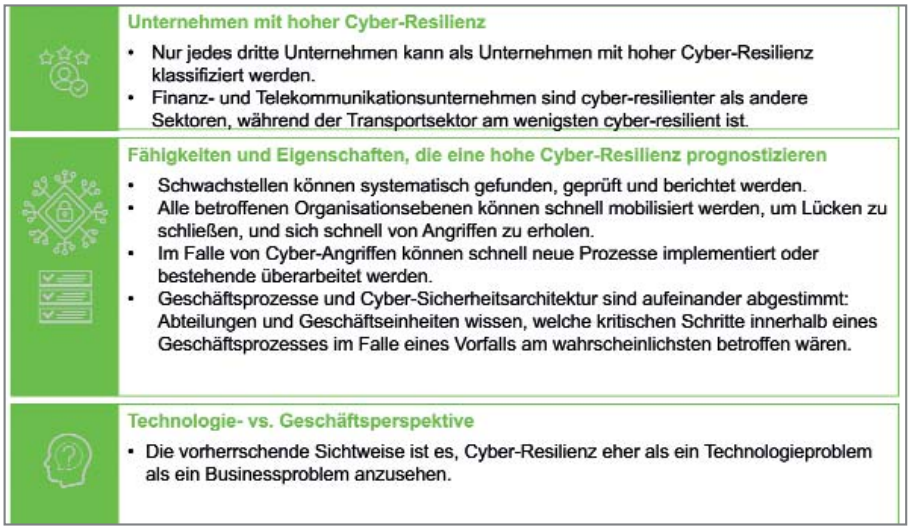
Bei TK-Providern interessieren sich Angreifer vor allem für die Zugangsserver, ihre Übertragungsnetze und deren Systeme. Im Zuge von All-IP findet ein Vereinheitlichen von Kommunikationsnetzen und Serversystemen statt. Hacker können mit einer Attacke auf das IP-Netz viele Dienste auf einen Schlag kompromittieren. Zeitkritische IoT-Anwendungen (Internet of Things) erhöhen daneben die technische Komplexität und stellen neue IT-Sicherheitsanforderungen. Ebenso erschwerend: In TK-Infrastrukturen sind häufig viele verschiedene Unternehmen und Subunternehmen beteiligt, was oft verschachtelte Verantwortlichkeiten nach sich zieht. Unter diesen Umständen wird es schwer, ein durchgängiges Schutzniveau zu etablieren.

Energieversorger und TK-Unternehmen können hier auch exemplarisch für viele weitere Marktteilnehmer stehen. Einerseits brauchen wir die immer stärkere Vernetzung und Digitalisierung vieler Wirtschaftszweige und öffentlicher Organisationen, andererseits entstehen dadurch neue Risiken und damit auch eine neue Verantwortung. Ihr können wir uns nur mit einer hohen digitalen Resilienz stellen, nicht nur die klassischen Kritis-Betreiber.

Unterschiedlich widerstandsfähige Kritis-Betreiber

Der Cyber Resilience Report zeigt, wie widerstandsfähig die Branchen im Vergleich aufgestellt sind. Über alle Länder hinweg sind Finanz- und TK-Unternehmen (46 %) am besten gegen Cyberangriffe gerüstet. Es folgen die Sektoren Wasser (36 %), Gesundheit (34 %) und Energie (32 %). Bei Transportunternehmen erreichen nur 22 % ein hohes Resilienzniveau.

Die befragten Entscheider betrachten die Cyberresilienz eher als ein Technikproblem. Im TK-Sektor sollten Geräte in einem Netz intensiv auf Schwachstellen überwacht werden. Die Energieversorger identifizieren dagegen die digitale Mess- und Regeltechnik, die auf ICS- und Scada-Geräten basiert, als den potenziellen Angriffspunkt.



Ergebnisse des Cyber Resilience Survey *(Quelle: Greenbone)*

Welche Fähigkeiten machen hochresilient?

Branchenübergreifend veranschaulicht der Report, worin sich die hochresilienten Unternehmen von denen unterscheiden, die sich auf einem geringeren Resilienzlevel bewegen. Demnach hängt die Widerstandsfähigkeit entscheidend von diesen vier Schlüsselkriterien ab:

- Schwachstellen können systematisch gefunden, geprüft und berichtet werden.
- Alle betroffenen Organisationsebenen können schnell mobilisiert werden, um Lücken zu schließen und sich schnell von Angriffen zu erholen.
- Im Fall von Cyberangriffen können schnell neue Prozesse implementiert oder bestehende überarbeitet werden.
- Geschäftsprozesse und Cybersicherheitsarchitektur sind aufeinander abgestimmt.

In einem weiteren Analyseschritt zeigt die Studie, wie Unternehmen mit diesen und weiteren Fähigkeiten ihr Resilienzniveau deutlich steigern können (*Bild*).

Cyberresilienz ist im Top-Management angesiedelt

Auch wenn die Auswirkungen von Cyberattacken mit der immer weiter fortschreitenden Digitalisierung auch stärker die Geschäftsprozesse betreffen: Cyberresilienz wird von den befragten Unternehmen immer noch als eine im Wesentlichen technische Herausforderung angesehen. Die Aufgabe der Unternehmensführungen ist es, die Ganzheitlichkeit digitaler Resilienz zu verstehen.

Nur wenn das Thema Cyberresilience auch in der Leitungsebene fest verankert ist, haben die Unternehmen gute Chancen, gegen die täglichen Bedrohungen zu bestehen. Dabei ist eine Fokussierung auf die wichtigsten und kritischsten Assets und Geschäftsprozesse wichtig und hilfreich. Am Ende kann eine Organisation jedoch nur durch eine gelebte Kultur der Sensibilität gegenüber den Risiken, mit guten Prozessen und wirksamen technischen Mitteln ausgestattet, eine gute Cyberresilience erreichen. *(bk)*