Digitalisierung ja – aber nicht ohne Cyber Resilience

WIDERSTAND Die Digitalisierung hat neben vielen Vorteilen einen gewichtigen Nachteil: Das Risiko von Cyberattacken steigt – und zwar deutlich. Deshalb ist es wichtig, seine Cyber Resilience auf allen Unternehmensebenen zu stärken und sich nicht nur auf immer höhere Sicherheitsmauern zu verlassen.

AUTOR THOMAS MEIER

Beim Thema Digitalisierung wird oft zu wenig an die Sicherheit gedacht – ein fataler Fehler. Denn jede Entwicklung und jedes Konzept – egal ob Industrie 4.0, IoT, As-a-Service-Modelle usw. – lösen automatisch Sicherheitsfragen aus. Hinzu kommt, dass Angreifer immer effizienter und professioneller arbeiten. So dauert es nicht selten Wochen oder gar Monate, bis ein Angriff entdeckt wird. Deshalb ist es unerlässlich, mehr in die Erkennung und Reaktion auf Cyberattacken zu investieren.

Ein systematischer Sicherheitsansatz ist das A und O erfolgreicher Cyber Security. Dabei müssen sowohl das Risikomanagement, der Schutz der Informationen, die Erkennung und Reaktion auf Sicherheitsvorkommnisse als auch die Wiederherstellung und Optimierung berücksichtigt werden.

Cyber Resilience ist die Stärkung der Widerstandskraft gegen Cyberattacken. fotobyline

STÄRKEN SIE IHR SICHERHEITS-IMMUNSYSTEM

In der Cyber Security verhält es sich wie bei einer Grippe: Es ist praktisch unmöglich, alle (Cyber-)Viren einzufangen, jedoch kann das Ausmass der Grippe dank einem starken Immunsystem eingedämmt werden. So ist auch der Auf- und Ausbau zielgerichteter Massnahmen zur Stärkung der Widerstandskraft gegen Cyberattacken (Cyber Resilience) unabdingbar. Damit das gelingt, muss Cyber Resilience im Management wahrgenommen und entsprechend umgesetzt werden.

Cyber Resilience bedeutet aber nicht, nur die Sicherheitsmauern ständig zu erhöhen. Zum einen kommt der Architektur des Unternehmensnetzwerks eine wichtige Bedeutung zu. Zum anderen geht der Trend klar in Richtung einer intensiveren Überwachung der Sicherheitssysteme sowie der Erkennung von Vorfällen, wie es auch das NIST Cyber Security Framework empfiehlt. Eine simulierte Cyberattacke kann hier wertvolle Erkenntnisse liefern. Es braucht aber auch neue Sicherheitsansätze, bei denen die Detektion und Reaktion auf Angriffe im Vordergrund stehen. Der Ansatz hier lautet: agieren statt reagieren.

CYBER DEFENCE ALS 24X7 AUFGABE

Cyberattacken lassen sich nicht verhindern. Deshalb ist die Erkennung, Analyse und Reaktion auf Cyberangriffe umso wichtiger – und zwar 24x7. Genau hierfür ist ein Cyber Defence Center zuständig, das auch aktiv nach Bedrohungen und potentiellen Angriffen sucht. Deshalb basiert Cyber Defence nicht nur auf einer defensiven, sondern insbesondere auch auf einer offensiven Strategie. Das bedeutet konkret: Während sich das offensive Team (Red Team) auf die Simulation eines Angriffs fokussiert, konzentriert sich das defensive Team (Blue Team) auf die Abwehr. Die beiden «rivalisierenden» Gruppen haben zwar unterschiedliche Aufträge und Aufgaben, verfolgen aber dennoch ein gemeinsames Ziel: die Cyber Security des Unternehmens zu optimieren.

Moderne Cyber Security verlangt somit nicht nur hohe Schutzmauern, sondern auch eine starke Cyber Resilience. So können Sie Ihr Unternehmen nachhaltig schützen – auch im Zeitalter der zunehmenden Digitalisierung.

DER AUTOR

Thomas Meier ist CEO der InfoGuard AG. Sein aktueller Beitrag steht im Rahmen der Partnerschaft zwischen der Chief Digital Community – Das KMU-Netzwerk für die Digitalisierung – und der UNTERNEHMERZEITUNG.
www.chiefdigital.ch