SIMPLYIT
LANWORKS

WIR MACHEN EXPERTENWISSEN WIRKSAM

www.lanworks.de

Cyber-Resilienz – Bullshit Bingo?

Stärken Sie das Immunsystem Ihres Unternehmens.

Alles nur Bullshit-Bingo? Nach Cyber-Security, Cyber-Defense, Cyber-Crime und Cyber-War nun also „Cyber-Resilienz“? Ist das der neue Stern am Cyber-Hype-Himmel? Was genau soll Cyber-Resilienz denn sein? Alter Wein in neuen Schläuchen? Oder ist das wirklich neu? Letztendlich ist Cyber-Resilienz für uns sowohl Erweiterung als auch eine Teildisziplin der IT-Sicherheit. Denn auch mit den besten IT-Sicherheitstools lassen sich Risiken nie wirklich vollständig verhindern. Man muss damit umgehen, also “managen”. Für eine echte Widerstandskraft muss man sich über mögliche Risiken im Klaren sein. Nur wer gut vorbereitet ist, kann Bedrohungen schnell erkennen, angemessene Maßnahmen ergreifen und den Schaden im besten Fall im Rahmen halten. Doch wie genau lässt sich die Widerstandskraft von Unternehmen erhöhen? Welche Technologien sind die richtigen und welche Rolle spielt ein leistungsstarkes Identity- und Access Management dabei?

Stärken Sie das Immunsystem Ihres Unternehmens.

Lanworks AG
IT Engineering • IT Training & Coaching
Fürstenwall 41 • 40219 Düsseldorf
Fon +49 211 95059-69

Cyber-Attacken sind in gewisser Weise vergleichbar mit einem Virus. Egal wie gut die eingesetzten Technologien auch sind - einen Angriff bzw. eine Ansteckung wird man nie vollständig vermeiden können.

Ist man aber geimpft, dann hat das menschliche Immunsystem die passende Antwort, dann ist unsere Gesundheit zumindest vor schweren Verläufen geschützt. Ähnlich sehen wir das auch bei Cyberangriffen. Wenn man sie schon nicht gänzlich verhindern kann, dann gilt es, zumindest die Angriffsfläche zu verkleinern. Also Prozesse zu etablieren und Systeme zu härten, um auch in Krisensituationen gelassen reagieren zu können und betriebsfähig zu bleiben. Aber wie kann die Immunabwehr gestärkt werden? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist in seinem aktuellen Bericht zur IT-Sicherheit dabei auf einen ganz wichtigen Punkt hin: den immer bedeutsameren Schlüsselfaktor Resilienz.

Warum Cyber-Resilienz so wichtig ist – die IT widerstandsfähig machen und handlungsfähig bleiben.

Resilienz (von lateinisch resilire „zurückspringen, abprallen“) steht im Allgemeinen für die Widerstandskraft von Menschen und Unternehmen bei der Bewältigung von Krisensituationen.

Bezogen auf die IT verstehen wir Resilienz als Fähigkeit, sich auf schadhafte Situationen einstellen und diesen gezielt entgegenwirken zu können. Und das unabhängig davon, ob mutwillig, oder unbeabsichtigt oder durch die eigenen Mitarbeiter verursacht. Primär geht es doch darum, den Betriebsablauf und die betrieblichen Prozesse während eines Angriffs weiterhin sicherstellen zu können. Damit geht Cyber Resilienz weit über reine Cyber Security Strategie hinaus. Aus unserer Sicht eher ein “Mindset”, eine Haltung; ein übergreifendes, eher strategisch ausgerichtetes Konzept. Neben Maßnahmen**, Angriffe zu vermeiden**, gilt es grundsätzlich, **die eigenen Schwachstellen selbst aufzuspüren und zu bewerten, bevor es andere tun.** Risiken bewerten, klassifizieren und mögliche Gegenmaßnahmen **schon im Voraus zu ergreifen.**

Schützen – Entdecken – Entwickeln: die drei Säulen einer Cyber-Resilienz Strategie.

Bei der Umsetzung oder Einführung einer Cyber-Resilienz sollten aus unserer Sicht die folgenden Bereiche im Fokus stehen:

1. **Ein guter Schutz für alle Identitäten, Apps und Daten**

Der Schutz Ihrer Systeme, Anwendungen und Daten ist von zentraler Bedeutung. Dabei stellt sich immer die Fragen: Wer bist Du, was darfst Du, wer hat Dir das für wie lange erlaubt? Jede Person (Identität) innerhalb einer Organisation (Mitarbeiter, Lieferanten, Kunden) benötigt, je nach Position oder Aufgabe, bestimmte Zugänge und Berechtigungen. Diese sollten nicht nur mit dem Mitarbeitereintritt vorhanden sein, sondern vorzugsweise automatisiert auch bei Austritt wieder entzogen werden. Manuell geregelte Zugriffsrechte werden leider viel zu oft vergessen. Ohne ein durchdachtes **Identity- und Access-Management-System** ist es dann kaum noch nachvollziehbar, welcher User wann welche Rechte für etwas benötigt und wie diese Zugriffsrechte überhaupt entstanden sind. So entstehen schnell schwerwiegende Compliance-Verstöße und Einfallstore für Kriminelle.

2. **Die schnelle Aufdeckung**

Neben den präventiven Maßnahmen bildet eine schnelle Aufdeckung von Angriffen den zweiten Teil einer guten Cyber-Resilienz-Strategie. Laut einer Studie von IBM dauert es im Schnitt unglaubliche 206 Tage, bis eine Sicherheitsverletzung entdeckt wird. Ein langes Zeitfenster für umtriebige Angreifer, ohne dass jemand davon etwas mitbekommt. Damit Sie Sicherheitsrisiken adäquat erkennen können, muss man verstehen, welche Daten man hat, wo sie sich befinden und wie sie zu klassifizieren sind. Enorm hilfreich ist es auch, das individuelle Benutzerverhalten seiner Anwender zu kennen und zu verstehen. Denn nicht alle Verletzungen beginnen mit einem Angriff von außen. Vieles beginnt von innen. Weiß man aber, was eine "normalen" Aktionen eines Anwenders ist, dann ist es viel einfacher, ungewöhnliche Verhaltensweisen zu erkennen.

3. **Das Entwickeln einer guten Strategie** – **ändern Sie das Spiel zu Ihren Gunsten**

Mit einer aktiven und fortlaufenden Anpassung der Strategie sind Sie immer einen Schritt voraus. Ein statischer Ansatz, bei dem Prozesse und Vorgehensweisen einmalig definiert werden, ist morgen schon alt. Er reicht angesichts hochdynamischer Sicherheitsrisiken heute nicht mehr aus. Neue Angriffsvektoren werden heute durch Bedrohungsmodellierung vorhergesehen. Mit guten Simulationen und regelmäßigen Analysen werden die eigenen Lösungen fortlaufend auf ihre Wirksamkeit überprüft.

Tipps für die praktische Umsetzung: Die Resilienz in der Unternehmenskultur verankern.

Eine gute Widerstandskraft gegen Angriffe steht und fällt mit einer gelebten **Sicherheits-Kultur**. Denn der beste Plan ist nur so stark wie seine schwächste **Stelle**. Das Öffnen des falschen E-Mail-Anhangs oder die Verwendung eines USB-Sticks – gerne getarnt als hübsches Werbegeschenk – ist nicht selten der Anfang einer großen Katastrophe. Daher sollten sich alle im Unternehmen darüber im Klaren sein, dass diese potenziell eine große Gefahr darstellen. Hier ist eine kontinuierliche **Sensibilisierung** erforderlich. Eine clever durchdachte Kommunikation schafft ein nachhaltig geprägtes Bewusstsein für die konkreten Gefahren. Eine wirksame Maßnahme in diesem Zusammenhang sind gezielte **Mitarbeiterschulungen und spezielle Workshops.**

Fazit

Technologie allein schafft noch keine Resilienz. Regularien und IT-Compliance zeigen weder Schwachstellen auf, noch werden Angriffe verhindert. Ungeschulte Mitarbeiter werden häufig nicht als erste Verteidigungslinie gesehen, da die notwendige Sensibilisierung und Aufmerksamkeit fehlen. Folglich ist neben der Technologie und einer sauberen Compliance vor allem die Sicherheitskultur ein wichtiges Zahnrad im komplexen Gesamtkontext einer echten Cyber-Resilienz.

Wie kann die Lanworks helfen?

Als IT-Systemhaus mit über 30 Jahren Erfahrung und mit Expertenwissen für Identity- und Access Management (IAM) unterstützen wir bei der strategischen Planung, der Umsetzung und dem Betrieb von modernen und effizienten IT-Lösungen rund um die Verwaltung von Identitäten und Zugriffen. Unsere Berater zeigen Ihnen, wie Ihr IAM auch im Krisenfall reibungslos funktioniert. Für uns bedeutet das: Die täglichen Aufgaben souverän meistern und im Ausnahmefall gelassen reagieren. Möchten Sie mehr dazu erfahren?

Ansprechpartner: Dipl.-Kfm. Georg W. Rösch

Lanworks AG
IT Engineering • IT Training & Coaching
Fürstenwall 41 • 40219 Düsseldorf
Fon +49 211 95059-69