MENT IQ

Effektive Cyber-Vorsorge

Cyber Recovery als Schlüssel für mehr Cyber Resilience

MEDIALINE GROUP

Cyber-Angriff: Die Frage ist nicht „ob“, sondern „wann“

Die Sicherheitslage ist prekär, Daten aus unterschiedlichsten Quellen bestätigen es: Jedes zehnte Unternehmen in Deutschland wurde im vergangenen Jahr Opfer eines Cyberangriffs – das geht aus einer Umfrage im Auftrag des TÜV-Verbands hervor. Auch der Threat Hunting Report 2023 zeichnet ein düsteres Bild. Das Ergebnis hier: die interaktiven Angriffsversuche seien im Vergleich zum Vorjahr um weitere 40 Prozent gestiegen. Der BKA-Bericht gibt an, dass sich die Schäden durch IT-Attacken in Deutschland im Jahr 2022 auf 203 Milliarden Euro beliefen und komplettiert damit den Umriss der Lage.

Die größten Bedrohungsherde im virtuellen Raum? Neben der organisierten Cyberkriminalität durch hacktivistische oder auch staatliche Akteure können sogenannte Innentäter, also aktive oder ehemalige Mitarbeiter Unternehmen zum Verhängnis werden. Auch der russische Angriffskrieg hinterlässt seine Spuren im Cyberraum. Die Anzahl der Cybervorfälle gegen deutsche Unternehmen ist seit Eskalation des Konflikts merklich gestiegen. Und dabei ist der immense Business Impact von beispielsweise Ransomware-Attacken weithin bekannt. Ob Entlassungen von Personal, wirtschaftlicher Totalausfall oder monetärer Schaden in Millionenhöhe – die Liste ist lang. Die Frage, die sie sich stellen sollten, lautet demnach nicht „Werde ich angegriffen?“, sondern „Wann?“. Und mit dieser Erkenntnis raten wir dringend dazu, Cyber-Recovery als Ihr höchstes Gut zu betrachten.

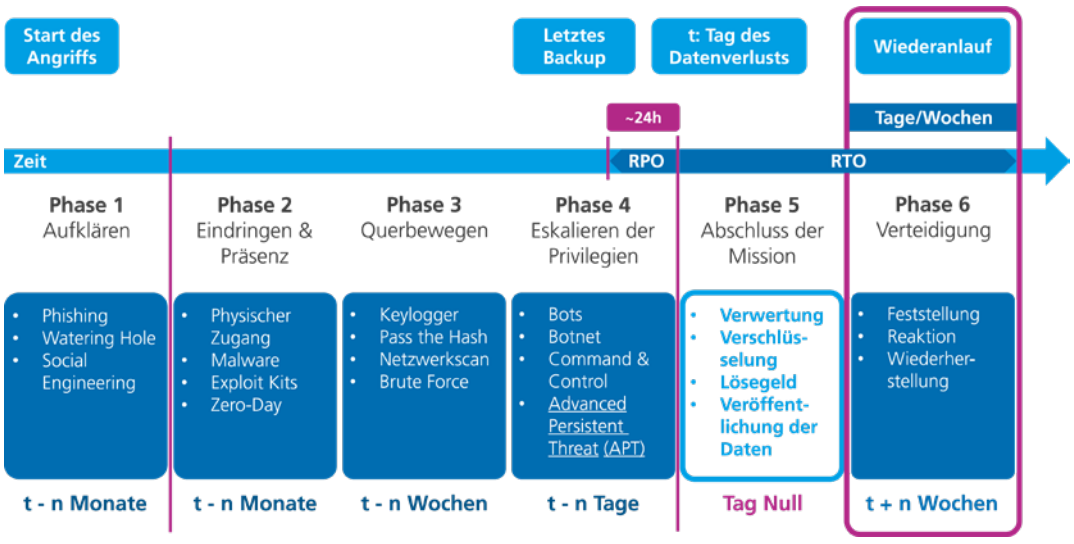
MENT IQ

Cyber-Resilience durch Cyber-Recovery

Mit dieser düsteren Grundannahme wird klar: Vorbeugende Maßnahmen sind enorm wichtig. Fälschlicherweise wird diese Vorsorge meist überwiegend im Bereich der Gefahrenabwehr getroffen und selten in die Recovery-Fähigkeit investiert. Dabei können kleine Schritte der Absicherung bereits große Effekte erzielen.

Vorsorge mit Hilfe eines zuverlässigen Cyber Recovery Konzepts ist laut unseren Experten die erste und wichtigste Handlung für mehr Cyber-Resilience,

- … um nicht erpressbar zu sein
- … um sich extern absichern zu können.



Die Anatomie einer Attacke

Vorbeugende Maßnahmen, die Sie für die Erhöhung Ihres Cyber Schutzniveaus vornehmen können, beziehen sich jeweils auf die einzelnen Phasen einer Attacke. Aus langjähriger Erfahrung wissen wir: in puncto IT Security gibt es keine hundertprozentige Sicherheit!

Darum empfehlen wir mit Vorkehrungen für die letzte Phase zu starten. Somit sind sie - wie der Trapezkünstler vor dem Fall - mit einem dichten Sicherheitsnetz ausgestattet.

MENT IQ

Cyber-Recovery statt Lösegeld

Interessant wird es bei der Thematik rund um Lösegeldzahlungen. Im Schnitt wurden 80 Prozent der Unternehmen, die diesen Forderungen nachgingen, ein zweites Mal Opfer eines Angriffs. 78 Prozent der Unternehmen, die wiederum nicht zahlten, konnten ihre Daten vollständig herstellen. Lösegeldzahlungen verweigern ist statistisch gesehen also der bessere Weg. Die Kosten für Cyber-Vorsorge sind in jedem Fall geringer, als die kombinierten Kosten für Lösegeld und die dazugehörigen Bereinigungs-Aufwände, insbesondere bei multiplen Angriffen.

Fit für die Cyberversicherung

Einen wichtigen Teil der Cyber-Vorsorge stellt die Cyberversicherung dar. Denn Cyberversicherungen sind mittlerweile nicht mehr Teil der allgemeinen Unternehmenshaftpflicht oder Betriebsunterbrechungsversicherung. Denn auf Seiten der Versicherungen steigen die Kosten. Neben schwer einschätzbarem Angriffsrisiko und hohen Bereinigungskosten gesellt sich die erhöhte Anfälligkeit von Unternehmen für Cyber-Attacken – wegen der gestiegenen Cloud-Nutzung. Der Weg zur Cyberversicherung setzt eines voraus: Unternehmen müssen sich bei den Versicherungsgebern „qualifizieren“, beispielsweise durch folgende Vorsorgemaßnahmen:

- Patch Management, Software + OS-Updates
- Aktuelles, getestetes und geschütztes Offline-Backup
- Schnelligkeit der Wiederherstellung
- Erfordernis von Lösegeldzahlungen
- 2-Faktor Authentifizierung, Art der Cloud Nutzung
- Endpoint Protection und Managed Detection & Response (E-/XDR, MDR)

MENT IQ

Wie steht es um Ihre Recovery-Fähigkeit?

Mit Ihrer „Recovery-Fähigkeit“ stellen Sie sicher, dass sie im Fall von Datenverlusten handlungsfähig bleiben, indem Sie die Daten wiederherstellen können, die Sie für Ihren Geschäftsbetrieb benötigen. Dabei unterscheiden wir zwischen drei aufeinander aufbauenden Kategorien:

Grundsätzliche Restore-Fähigkeit:

Die Backupumgebung sowie das Wissen der Mitarbeitenden ermöglicht die grundsätzliche Wiederherstellung der gesicherten Daten.

Desaster Recovery-Fähigkeit:

Die Redundanz in der Datenhaltung sowie die Backup-Architektur ermöglichen eine Wiederherstellung der Backupumgebung im Desaster-Fall. Die Backup-Administratoren haben das nötige Wissen, die Durchführung wird regelmäßig geprobt.

Cyber-Recovery-Fähigkeit:

Eine vollständige Cyber-Recovery-Umgebung ist implementiert. Gesicherte Daten liegen in unveränderlicher Form in einem Cyber-Vault vor und sind durch ein „Air-Gap“ vom produktiven Netz getrennt. Zusätzlich existiert eine Cyber-Recovery Infrastruktur, die gesicherte Daten analysiert, und so deren Integrität sicherstellt. Im Ernstfall dient der Cyber Vault als „Reinraum“ für die Aktivitäten von Forensikern und Strafverfolgungsbehörden und ermöglicht Recovery-Tests in einer abgeschotteten Umgebung. Ein Netzwerk an unterstützenden Partnern steht zur Verfügung.

Cyber-Recovery Score Card

Mit der Score Card bewertet mentIQ Ihre Cyber-Recovery-Fähigkeit. Anhand eines pragmatischen, individuellen Assessments werden die drei verschiedenen Recovery-Fähigkeiten ausgemacht. Außerdem wird Organisation, Architektur, Datenhaltung und Restore-Vorsorge überprüft. Zudem geben Ihnen unsere Experten eine Empfehlung zur Weiterentwicklung Ihrer IT-Umgebung mit auf den Weg. So können Sie im Fall eines Cyber-Angriffs nicht nur auf Lösegeldzahlungen verzichten, sondern sind auch mit den nötigen Maßnahmen ausgestattet, um sich für eine Cyberversicherung zu qualifizieren. Dabei gilt: auch kleine Schritte können die Sicherheit bereits signifikant erhöhen. Zögern Sie also nicht, denn die Frage ist nur „wann“.

Kontakt:
Günter Maier, Geschäftsführer mentIQ

Ihr Partner für intelligentes Datenmanagement. Wir betreuen Sie erstklassig, hochprofessionell und auf Augenhöhe. Gerne gehen wir mit Ihnen gemeinsam eine effektive Cyber-Recovery Strategie an. Kontaktieren Sie unseren Recovery-Spezialisten Günter Maier unverbindlich für ein erstes Beratungsgespräch:

E-Mail: guenter.maier@mentiq.com
Telefon: +49 89 95 415 72 50