Gemeinsam gegen Cyber-Risiken

Die aktuelle Bedrohungslage durch Cyberangriffe steigt unaufhaltsam. Fast schon täglich ist der Presse zu entnehmen, dass wieder ein Unternehmen gehackt wurde und dadurch über Wochen handlungsunfähig ist. Dabei ist die Finanzbranche ein attraktives Ziel.

In 2023 wurden pro Tag 250.000 neue Schadprogamm-Varianten identifiziert. Allein diese Zahl macht deutlich, dass es extrem aufwendig ist, einen Angriff zu identifizieren, geschweige denn, ihn abzuwehren. Es liegt auf der Hand, dass wir in der Genossenschaftlichen FinanzGruppe hier einen Vorteil haben: Das gemeinsame Vorgehen macht den Unterschied und sichert am Ende den Betrieb – trotz Notfall. Wie das in der DZ CompliancePartner GmbH aussieht, soll im Folgenden skizziert werden.

Was tun, wenn der Notfall eintritt

Spielen wir das doch mal durch: Was passiert, wenn der Notfall eintritt?

Der erste Impuls ist, sich zu fragen, welche Daten konkret betroffen sind und wo sie genau liegen. Welche Systeme und Prozesse hat es erwischt? Wird es Folgeschäden geben und welches Ausmaß wird am Ende der Datenschutzvorfall haben? Als betroffenes Unternehmen versucht man sich zunächst einen Überblick zu verschaffen, um den Schaden und die davon ausgehenden Risiken einschätzen zu können – um dann in einem zweiten Schritt entsprechende Gegenmaßnahmen zu starten.

Aber: Ist das dann überhaupt noch möglich? Was kann das Unternehmen leisten, wenn es nicht mehr auf seine IT zugreifen kann? Die Feststellung des Schadens erscheint fast als das geringste Problem. Die Frage ist dann schlicht: Wie können die vertraglichen, aber auch regulatorischen Pflichten in einer solchen Situation noch erfüllt werden? Glücklich ist, wer rechtzeitig Sicherheitsvorkehrungen getroffen hat.

Aus IT-Sicht steht der Ausfall einzelner Anwendungen oder des Rechenzentrums im Zentrum der Überlegungen. In der Regel greifen die Sicherheitsregelungen und Fall-Back-Lösungen des Business Continuity Management (BCM) – bei uns in der DZ CompliancePartner GmbH sind das u. a. Redundanzen im IT-Betrieb, vertragliche Vereinbarungen zu Wiederherstellzeiten, Notfallnummern, Notstrom und vieles mehr.

Und wenn es noch schlimmer kommt?

Was ist, wenn alle Verbindungen zu den IT-Systemen getrennt, alle Server, alle Leitungen, alle Rechner abgeschaltet werden müssen? Was ist dann zu tun?

Diese Fragen haben wir in der DZ CompliancePartner GmbHuns nicht nur gestellt, weil es in den MaRisk, den BAIT und auch in DORA gefordert ist. Wir haben sie uns gestellt, weil das die Realität bei angegriffenen Unternehmen wurde und wir dazu eine Antwort haben wollen und müssen: Wie können wir unsere Dienstleistung erfüllen, sollten wir einen „Black Screen Day“ haben.

Ein Blick ins Notfallhandbuch auf die zeitkritischen Prozesse ist dabei nur eingeschränkt hilfreich. Es geht darum, den Mitarbeiterinnen und Mitarbeitern der DZ CompliancePartner GmbH möglichst schnell wieder ihre Aufgabenerfüllung zu ermöglichen, damit wir letztlich unseren Verpflichtungen gegenüber unseren Kunden nachkommen können. Und das im schlimmsten Fall parallel und unabhängig von der ggf. notwendigen Neu-Inbetriebnahme der IT, die – und auch damit muss man rechnen – unter Umständen mehrere Wochen andauern kann.

In der DZ CompliancePartner GmbH setzen wir – zusätzlich zum BCM – auf eine dreifache Absicherung:

1. Alle Notfallnummern sind analog und zudem lokal auf Firmenhandys verfügbar, der Austausch untereinander ist möglich.
2. Die Zusammenarbeit mit der Atruvia ermöglicht, zeitkritische Prozesse in der Dienstleistungserbringung über den Bankenarbeitsplatz durchzuführen.
3. Ein Pool von Ersatz-Hardware ermöglicht den schnellen Austausch infizierter Geräte und damit eine zügige Weiterarbeit.

1. Verfügbarkeit von Notfallnummern

Die DZ CompliancePartner arbeitet nahezu papierlos und über ganz Deutschland verteilt. Aber an den Standorten steht selbstverständlich der papierhafte Notfallordner. Zugriff darauf haben in erster Linie die Mitarbeiterinnen und Mitarbeiter, die an den Standorten bzw. in deren Nähe arbeiten.

Für alle anderen Mitarbeiter haben wir eine Lösung geschaffen, die einen gesicherten Zugriff auf die wichtigsten Kontaktdaten und Informationen auf Firmengeräten – z. B. Handys – ermöglicht. Die Daten werden dabei lokal auf den Geräten zur Verfügung gestellt. Ein Prozess sichert die Aktualität der Daten und eine entsprechende firmeninterne Kommunikation samt Arbeitsanweisung

klärt die Mitwirkungspflichten der Mitarbeitenden – beginnend mit der aktiven Nutzung des Firmenhandys bis hin zu regelmäßigen Updates.

2. Verfügbarkeit eines dezentralen Zugriffs über Atruvia-Anwendungen

In der Zusammenarbeitsbeziehung zu unseren Kunden nutzen wir – wo immer es machbar ist – die Möglichkeiten, die Atruvia zur Verfügung stellt. Dadurch, dass sie ihre Anwendungen zum großen Teil Agentur-fähig bereitstellt, sind unsere Beauftragten immer auch als Mitarbeiter des jeweiligen Kunden eingerichtet: Das heißt, sie haben eine User-ID der jeweils betreuten Bank. Zudem können wir bereits seit längerem bei einigen Banken über den Bank-managed-Client einer Bank direkt auf die Anwendungen der Bank zugreifen.

Mit Blick auf das Notfallszenario sind diese modernen Technologien eine große Hilfe. Über den Weg der Atruvia-Anwendungen ist der Zugriff auf die benötigten Mandantendaten auch im Notfall gewährleistet. Damit sind wir in der Lage, den rechtlichen Verpflichtungen nachzukommen und insbesondere (zeit)kritische Prozesse zu bearbeiten.

Für die internen Prozesse im Rechnungswesen und in der Personalabteilung haben wir ebenfalls ein entsprechendes Notfallkonzept hinterlegt. So sind wir auch hier schnell in der Lage, den Mitarbeitenden Zugriffe auf die Buchhaltungsdaten, jenseits der „normalen" Infrastruktur, zur Verfügung zu stellen.

3. Verfügbarkeit von Ersatz-Hardware

Zu guter Letzt halten wir (Ersatz-)Hardware vor, die im „worst case" schnell ausgerollt werden kann. Das sind Notebooks, die schnell mit einem Image bespielt und an die Mitarbeiter ausgegeben werden können. Für diese „Grundbetankung" halten wir z. B. auch extra entsprechende USB-Sticks vor, um unabhängig vom Netzwerk zu sein.

Zusammengefasst haben wir Respekt vor dem Risiko eines Cyberangriffs. Selbst mit dem beschriebenen Plan in der Hinterhand werden die anfallenden Nacharbeiten und Umsetzungsschritte in den „Normalbetrieb" anspruchsvoll sein. Aber: Wir sehen uns gut aufgestellt mit unserem Notfallkonzept einerseits und der Zusammenarbeit mit Atruvia andererseits, über deren risikoorientierte und intelligente IT-Struktur der Betrieb auch im Notfall möglich ist.

Wenn Sie Fragen zu unserem Sicherheitskonzept haben, kommen Sie gerne jederzeit auf uns zu. ▬

Sandra Sitter
Bereichsleiterin IT & Projekte,
E-Mail: sandra.sitter@dz-cp.de