DerTreasurer
NACHRICHTEN FÜR DIE FINANZABTEILUNG
DEZEMBER | 2023

So bereiten sich Treasurer auf Cyberangriffe vor

Das Thema Cybercrime wird für Unternehmen zu einer wachsenden Bedrohung. Die Konsequenzen nach einem Angriff sind bitter. Das Treasury muss sich deshalb auf den Ernstfall vorbereiten. Wie muss man an „Tag X“ reagieren und wie sieht die Nachbereitung aus?

Die Zahl der Cyberangriffe auf Unternehmen steigt. Prävention wird immer wichtiger.

Beim diesjährigen „11. Cash Management Campus 2023“ in Köln hat DerTreasurer zusammen mit BNP Paribas mit den Teilnehmern in einem Workshop erarbeitet, was Treasurer über das Thema Cybercrime wissen sollten und wie sich Unternehmen vorbereiten können.

In diesem Whitepaper haben wir die Ergebnisse für Sie festgehalten. Zudem finden Sie eine Checkliste mit den wichtigsten Maßnahmen zur Vorbereitung auf einen Cyberangriff, was Unternehmen am „Tag X“ tun sollten und wie die Nachbereitung nach einem Angriff aussehen sollte. Zudem enthält das Whitepaper ein Interview mit dem Fachanwalt Lutz Martin Keppeler, Partner bei Heuking Kühn Lüer Wojtek, über bestehende Meldepflichten.

Erstellt wurde die Checkliste mit Hilfe des Inputs der Teilnehmer des „Cash Management Campus“ sowie von Andrej Ankerst (BNP Paribas), Lutz Martin Keppeler (Heuking Kühn Lüer Wojtek) und Carsten Meywirth (Leiter der Abteilung Cybercrime beim Bundeskriminalamt).

Checkliste

Vorbereitung, Maßnahmen Tag X, Nachbereitung

Vorbereitung und Maßnahmen

Notfallplan erstellen

— Es sollte ein Notfallplan vorliegen, der beschreibt, was bei einem Ernstfall zu tun ist. Im Plan sollte stehen,
  - welche Schritte das angegriffene Unternehmen in welcher Reihenfolge tun sollte,
  - wer informiert werden muss,
  - wer für was verantwortlich ist.

  Zu beachten ist, dass der Notfallplan cybersicher sein und nicht auf einem Computer liegen sollte, der ggf. gehackt werden und auf den deshalb nicht zugegriffen werden kann. Besser ist es, den Plan bei einem Dienstleister zu hinterlegen und/oder in Papierform.
— Auch für alle ausländischen Tochtergesellschaften sollten Notfallpläne, Listen, Back-up-Szenarien etc. vorliegen; Ansprechpartner sollten definiert werden.

Vorbereitung der Organisation

— Regelmäßige Schulungen: Alle Mitarbeiter sollten informiert werden, wie die verschiedenen Arten von Cyberattacken aussehen.
— Simulationen durchführen: Der Druck bei einem Cyberangriff ist enorm. Um die Resilienz zu stärken, hilft es, zu üben und Situationen für den „Tag X" zu simulieren. Die Simulation dient auch dazu, Schwachstellen im eigenen Notfallplan zu entdecken und diese korrigieren zu können. Beispiel: Die Schließanlage des Betriebsgeländes wird zentral gesteuert. Was passiert, wenn die Systeme abgeschaltet werden?
— Versicherung abschließen: Unternehmen sollten prüfen, ob dies eine Option wäre. Wenn ja, sollten sie prüfen, welche Cyberrisikoversicherungen zur Verfügung stehen.

Kommunikationsfähigkeit sicherstellen

— Ausrüstung: Die IT-Infrastruktur sollte so aufgestellt sein, dass Mitarbeitern im Ernstfall vom Cyberangriff nicht betroffene Laptops und Handys zur Verfügung stehen.
— Interne Kommunikation: Hier kommt es auf die Geschwindigkeit an. Im Vorfeld sollte festgelegt werden, wer bei einem Angriff zuerst informiert werden muss. Es sollten Kontaktlisten (in Papierform oder auf einem USB-Stick) vorliegen.
— Externe Kommunikation: Wenn es zu einem Angriff kommt, sollte das Unternehmen diesen Angriff nicht verschweigen. Es gibt allerdings Ausnahmen, wenn ein Unternehmen zum Beispiel zur kritischen Infrastruktur gehört. Hier sollte die Kommunikationsabteilung eines Unternehmens im Vorfeld eine Strategie entwickeln, wie sie bei einem Cyberangriff berichten will (Notfall-Kommunikationsplan) und an wen sie berichten muss (Meldepflichten). Eine Maßnahme könnte zum Beispiel die Kommunikation über die Homepage sein, auf der Lieferanten, Kunden etc. informiert werden. Wer proaktiv kommuniziert, bekommt in der Regel auch mehr Verständnis.

Kontaktaufnahme und Vernetzung

— Persönliche Kontakte sind das A und O in solchen Fällen. Von allen Beteiligten (Kollegen, Bankern, TMS-Anbieter etc.) sollten den verantwortlichen Personen im Treasury die Kontaktdaten vorliegen. Zudem sollte bestimmt werden, welcher Kommunikationskanal genutzt wird, wenn Anrufe oder E-Mails über das firmeneigene System nicht mehr möglich sind. Eine Option könnte sein, zuvor mit den relevanten Partnern private E-Mail-Adressen oder Telefonnummern auszutauschen, um bei einer Cyberattacke miteinander kommunizieren zu können. Zu beachten ist, dass mit den Daten sensibel umgegangen werden muss und sie am besten in Papierform vorliegen sollten.
— Im Ernstfall braucht die Bank eine Sicherheit/Legitimation, um aktiv werden zu können und Zahlungen ausführen oder verhindern zu können. Hier kann es sinnvoll sein, im Vorfeld ein Codewort mit allen wichtigen Beteiligten, die einbezogen werden sollen, zu vereinbaren. Im Vorfeld sollte abgesprochen werden, wer solche Freigaben erteilen darf. Die größte Sicherheit bietet in solchen Fällen ein guter persönlicher Kontakt zu den externen Ansprechpartnern.
— Etwaige Meldepflichten bei Behörden und Informationspflichten gegenüber Vertragspartnern sollten bekannt sein.

Zahlungsfähigkeit sicherstellen

— Die wichtigsten Zahlungen, die ein Unternehmen zu leisten hat, sollten vorab identifiziert werden. Entsprechende Listen mit allen wichtigen Überweisungsdaten sind wichtig, zum Beispiel Gehaltslisten oder die Bankdaten der wichtigsten Lieferanten. Die Liste sollte nicht auf einem Computer liegen, der womöglich gehackt und nicht genutzt werden kann. Die Listen können in Papierform oder auf einem USB-Stick in einem Tresor oder zu Hause aufbewahrt werden. Auch können historische Zahlungsdateien in einer separaten Umgebung, wie der Cloud, archiviert werden.
— Wenn ein E-Banking-Back-up-System aufgesetzt wurde, sollte dieses regelmäßig genutzt werden, um zu kontrollieren, ob alles läuft und alle Daten aktuell sind (zum Beispiel Konten, Benutzer).

— Unternehmen sollten vorab überlegen, ob und wie sie ggf. Lösegeld zahlen. Es gibt Unternehmen, die in der Bilanz Rückstellungen für Cyberattacken bilden. Im Fall von Cyberattacken wird oft mit Kryptowährungen wie Bitcoin bezahlt.

Tag X

Schritte, wenn es zur Cyberattacke kommt

— Kontaktieren Sie sofort Ihren persönlichen Bankberater. Sollten unautorisierte Zahlungen unterwegs sein, wird Ihre Bank die Empfängerbank bitten, den Geldfluss zu blockieren. Die Bank kann zudem eine Betroffenheitsanalyse durchführen.
— Sprechen Sie mir der IT-Abteilung und folgen Sie deren Anweisungen.
— Häufig ist der erste Impuls nach einem Angriff, alle E-Banking-Systeme zu sperren und alle Computer etc. in Quarantäne zu schicken. In einigen Fällen reicht es jedoch, etwa nur den Ebics-Zugang zu sperren und nicht das ganze E-Banking-System, vor allem wenn dieses nicht in der IT-Infrastruktur des Unternehmens läuft.
— Wenn eine Cyberversicherung vorhanden ist, sollte der Anbieter informiert werden.
— Erstatten Sie so schnell wie möglich Anzeige bei der Polizei, damit diese Ermittlungen aufnehmen und die flüchtigen, digitalen Spuren sichern kann. Wenden Sie sich dafür idealerweise an die Zentrale Ansprechstelle Cybercrime (ZAC) Ihrer Landespolizei. Die Kontaktdaten finden Sie unter www.polizei.de/zac oder über Ihre örtliche Polizeidienststelle. Für die Ermittlungen von Interesse sind in der Regel Malware Samples, IP-Adressen aus Logfiles, E-Mailadressen, von denen mit Ihnen kommuniziert wurde, jede Information zur Täterkommunikation sowie Hinweise auf Leak Pages.
— Beachten Sie die Fristen bei gesetzlichen Meldepflichten gegenüber Behörden und die Informationspflichten gegenüber einzelnen Vertragspartnern.

Nachbereitung

Lösegeld

— Bei einem Angriff wird in der Regel Lösegeld gefordert. Die Polizei rät grundsätzlich davon ab, Lösegeld zu bezahlen. Laut den Teilnehmern des „Cash Management Campus“ ist das Verhältnis zwischen denjenigen, die zahlen, und denjenigen, die nicht zahlen, relativ ausgewogen. Laut Daten des BKA zahlten 2022 rund 41 Prozent der betroffenen Unternehmen Lösegeld.
— Eine Lösegeldzahlung gibt Unternehmen keine Garantie, die Arbeitsfähigkeit tatsächlich wiederzuerlangen. Zudem sind Anschlusserpressungen nicht ausgeschlossen. Heimlich ausgeleitete Daten können dennoch beispielsweise im Darknet verkauft werden. Grundsätzlich befeuert laut der Polizei jede Lösegeldzahlung die Underground Economy und führt zu einer weiteren Zunahme von Cyberangriffen.
— In Sachen Lösegeldzahlung gibt es aber noch weitere Stolperfallen. International kann eine Ransomware-Zahlung als Terrorismuszahlung gewertet werden, beispielsweise in den USA. Je nach Angreifergruppe kann eine Lösegeldzahlung auch gegen internationales und EU-Sanktionsrecht verstoßen. Es muss also genauestens geprüft werden, ob das Unternehmen und die handelnden Manager sich nicht strafbar machen.

Kurz-Checkliste

Vorbereitung

— Notfallplan erstellen
— Vorbereitung der Organisation (Schulung, Tag X simulieren, Versicherung abschließen)
— Kommunikationsfähigkeit sicherstellen (Notfallausrüstung vorhalten, interne und externe Kontakte definieren, Strategien entwickeln, Meldepflichten beachten)
— Kontaktaufnahme und Vernetzung (Kontaktdatenlisten, Codewort, Legitimation klären, Liste mit Melde- und Informationspflichten)
— Zahlungsfähigkeit sicherstellen (Liste mit wichtigsten Überweisungsdaten, E-Banking-Back-up-System)
— alle Listen am besten in Papierform vorhalten oder auf einem USB-Stick in einem Tresor

Tag X

— persönlichen Bankberater kontaktieren
— Anweisungen der IT-Abteilung befolgen
— prüfen, ob E-Banking-System wirklich gesperrt werden muss
— Anzeige bei der Polizei erstatten
— ggf. Versicherung kontaktieren
— Fristen bei Meldepflichten bei Behörden sowie Informationspflichten bei Vertragspartnern beachten

Nachbereitung

— falls Lösegeld gezahlt werden soll, Sanktionsrecht genauestens prüfen
— Kommunikationsplan umsetzen
— betroffene Parteien auf dem Laufenden halten
— Zusammenarbeit mit anderen Parteien weiterführen (IT, Polizei etc.)

Kommunikationsplan umsetzen

— Der vorab entwickelte Kommunikationsplan muss greifen. Lieferanten, Kunden und Co. sollte das gehackte Unternehmen regelmäßig auf dem Laufenden halten. Auch nicht betroffene Kunden sollten informiert werden.
— Auch die eigenen Mitarbeiter müssen regelmäßig über den Stand der Dinge informiert werden, da die Verunsicherung in der Belegschaft während eines Cybervorfalls in der Regel hoch ist.

Zusammenarbeit mit anderen Parteien

— Die IT sollte informiert sein, wie wichtig welches System im Treasury ist und welches am schnellsten wieder freigeschaltet werden soll.
— Die Zeit nach einem Angriff sollte nicht unterschätzt werden, teilweise dauert es Monate, bis alle Systeme wieder freigegeben werden.
— Arbeiten Sie mit der Polizei und Forensikern zusammen, um das gesamte Ausmaß des Angriffs und dessen Folgen zu kennen. ←

Experteninterview

„Meldepflichten nicht vergessen"

Bei einer Cyberattacke müssen Unternehmen vieles beachten. Auch Melde- und Informationspflichten gehören dazu, sonst drohen Strafen. Ein Interview mit Lutz Martin Keppeler, Anwalt für Informationstechnologierecht und Partner bei HKLW.

Herr Keppeler, was sind nach einem Cyberangriff die ersten Schritte aus rechtlicher Sicht, die Unternehmen gehen sollten?
Es gibt gesetzliche Verpflichtungen, die Unternehmen beachten müssen. Diejenigen, die an der Börse gelistet sind, müssen die Anleger über eine Ad-hoc-Meldung informieren, wenn der Angriff kursrelevant sein könnte. Unternehmen der kritischen Infrastruktur haben eine Meldepflicht gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Datenschutzbehörde muss informiert werden, wenn die Angreifer personenbezogene Daten verschlüsselt oder entwendet haben. Zudem besteht teilweise auch eine Informationspflicht gegenüber einzelnen Vertragspartnern, vor allem in neueren Verträgen gibt es dazu eine Klausel, was im Falle eines Cyberangriffs passieren muss.

»Kommen Unternehmen ihren Meldepflichten nicht nach, drohen ihnen Bußgelder.«

Zunächst müssen Unternehmen die Notlage ja operativ bewältigen. Wie viel Zeit haben sie hinsichtlich der Melde- und Informationspflichten?
Es gibt unterschiedliche Fristen. Börsenunternehmen müssen innerhalb von 24 Stunden Bescheid geben. Die Datenschutzbehörde sollten Unternehmen am besten sofort, spätestens aber nach 72 Stunden informieren. Selbst wenn Unternehmen im Zweifel noch nicht das genaue Ausmaß des Angriffs kennen, sollten sie sich bei der Behörde melden. Unternehmen der kritischen Infrastruktur haben keine klare Frist. Die Unternehmen vergessen häufig, die Vertragspartner zu informieren, da gibt es meistens Fristen von Stunden bis zu wenigen Tagen.

Wie sehen die Konsequenzen aus, wenn Unternehmen den Pflichten nicht pünktlich nachkommen?
Prinzipiell drohen den Unternehmen Bußgelder in Millionenhöhe. Wenn sich ein Unternehmen trotz Meldepflicht bei den Behörden nicht meldet, könnte das Unternehmen bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes Strafgeld zahlen. Wie hoch die Strafe ist, wenn Geschäftspartner nicht informiert werden, kommt auf den jeweiligen Vertrag an.

Gibt es dafür schon Beispiele?
Ja, in Großbritannien musste ein Flugunternehmen, bei dem Personendaten gestohlen wurden, über 200 Millionen Pfund Bußgeld zahlen, weil es den Vorfall nicht rechtzeitig gemeldet hatte. In Deutschland habe ich solche hohen Summen allerdings noch nicht gesehen.

Werden die Behörden In Deutschland strenger?
Ich denke, ja. Vor rund fünf Jahren wussten sehr wenige Unternehmen, wen sie bei einem Cyberangriff informieren müssen. Das hat sich deutlich verbessert, denn durch die steigenden Zahlen wächst auch das Bewusstsein. Flächendeckend herrscht aber immer noch viel Unwissenheit. Schätzungsweise setzt sich bisher nur ein Drittel der deutschen Unternehmen im Detail mit Meldepflichten, Verträgen etc. auseinander.

Was sind dabei besondere Herausforderungen?
Die Meldepflichten einzuhalten ist besonders für Unternehmen mit mehreren Standorten kompliziert. Jedes Bundesland hat eine eigene Datenschutzbehörde: Es reicht nicht, dass der Mutterkonzern den Angriff meldet, sondern jede Gesellschaft muss sich an die Behörde des jeweiligen Bundeslands wenden. Bei Konzernen mit internationalen Standorten ist es sogar noch

komplizierter – in jedem Land, insbesondere außerhalb der EU, existieren andere Meldepflichten.

Zum Beispiel?
In den USA gelten etwa Sonderpflichten, wenn Kontodaten gehackt wurden. Das Unternehmen muss den betroffenen Personen ein halbes Jahr einen Service anbieten, bei dem das Konto über eine Software auf unregelmäßige Kontobewegungen überwacht wird. Unternehmen müssen sich auf solche Fälle vorbereiten und eine Liste mit den jeweiligen Maßnahmen und Kontaktdaten haben. An jedem Standort sollte es einen Ansprechpartner geben, der dafür zuständig ist.

Auch das Thema Lösegeld ist eine Herausforderung – manche Unternehmen zahlen, manche nicht. Haben Sie einen Tipp?
Gerade durch die Sanktionen, ausgelöst durch den Ukraine-Krieg, ist das Thema tückisch geworden. Die Zahl der Angreifergruppen aus Russland ist seitdem erheblich gestiegen. Wenn an solch eine Gruppe Lösegeld gezahlt wird, verstößt das Unternehmen gegen das Sanktionsrecht. Es reicht schon aus, wenn die Gruppe mit einem russischen Oligarchen assoziiert wird oder ein Zusammenhang vermutet wird. Es gibt nachrichtendienstliche Listen von der Polizei mit den Gruppen. Dabei ist ganz egal, in welcher Form gezahlt wird.

»Die Meldepflichten einzuhalten ist besonders für Unternehmen mit mehreren Standorten kompliziert.«

Was sollte man tun?
Zu beachten ist, dass Länder unterschiedliche Sanktionsrechte haben. Wenn Unternehmen Tochtergesellschaften im Ausland haben, müssen sie auf internationale Ebene prüfen, ob sie in einem Land gegen das Sanktionsrecht verstoßen. Es könnte sogar sein, dass Unternehmen sich in bestimmten Ländern mit der Zahlung an bestimmte Gruppen wegen Terrorismusfinanzierung strafbar machen. Das Problem ist: Hier schützt auch nicht immer eine Cyberversicherung, denn da gibt es häufig eine Klausel, dass

Lutz Martin Keppeler von Heuking Kühn Lüer Wojtek

die Versicherung nicht greift, wenn Unternehmen an solche Gruppen zahlen. Viele Unternehmen wissen nicht, dass sie sich strafbar machen.

Halten Sie Cyberversicherungen grundsätzlich für sinnvoll?
Grundsätzlich ja. Aber ich habe schon viele Fälle gesehen, bei denen die Versicherung nicht gegriffen hat oder nur einen Teil abgedeckt hat. Hier gibt es einige Streitfälle. Gerade bei hohen Summen sind die meisten Versicherer sehr streng. Generell ist es für Unternehmen schwer, so eine Versicherung überhaupt abzuschließen. Wegen der hohen Lösegeld-Summen, die dort fließen könnten, stellen die Versicherer viele Auflagen an die Unternehmen, zum Beispiel im Bereich IT.

Der Experte
Lutz Martin Keppeler ist Partner bei Heuking Kühn Lüer Wojtek. Er ist Fachanwalt für Informationstechnologierecht (Certified Specialist Lawyer for Information Technology Law).

Was bringt es dennoch?
Eine Versicherung kann für potentielle Versicherungsinteressenten sehr hilfreich sein. Die Versicherer sagen dann zum Beispiel, was das Unternehmen noch erledigen muss, um die Versicherung abzuschließen. So erhält das Unternehmen wertvolle Informationen, wo noch Nachholbedarf besteht. ←

Impressum: Verlag F.A.Z. BUSINESS MEDIA GmbH – Ein Unternehmen der F.A.Z.-Gruppe • **Redaktion** DerTreasurer, Pariser Straße 1, 60486 Frankfurt am Main, Telefon: (069) 75 91-32 52, E-Mail: redaktion@derTreasurer.de, Internet: www.derTreasurer.de • **Layout** Daniela Lenz, F.A.Z. BUSINESS MEDIA • **Haftungsausschluss** Alle Angaben wurden sorgfältig recherchiert und zusammengestellt. Für die Richtigkeit und Vollständigkeit des Inhalts von DerTreasurer übernehmen Verlag und Redaktion keine Gewähr. Für unverlangt eingesandte Manuskripte und unverlangt zugestellte Fotografien oder Grafiken wird keine Haftung übernommen. **Genderhinweis:** Wir streben an, gut lesbare Texte zu veröffentlichen und in unseren Texten alle Geschlechter abzubilden. Das kann durch Nennung des generischen Maskulinums, Nennung beider Formen („Unternehmerinnen und Unternehmer“ bzw. „Unternehmer/-innen“) oder die Nutzung von neutralen Formulierungen („Studierende“) geschehen. Bei allen Formen sind selbstverständlich immer alle Geschlechtergruppen gemeint – ohne jede Einschränkung. Von sprachlichen Sonderformen und -zeichen sehen wir ab.