Spotlight 11/24

DAS GRÖSSTE CYBER-RISIKO: DIE GEFAHR DURCH MENSCHLICHE FEHLER

Cyberkriminalität kann jeden treffen – ein vorbereitetes und durchdachtes Cyber-konzept ist für Schweizer Unternehmen zwingend notwendig.

Wenger Vieli AG
Dufourstr. 56
Postfach
8034 Zürich
—
Metallstr. 9
Postfach
6302 Zug
—
+41 58 958 58 58
spotlight@
wengervieli.ch

Die Cyberkriminalität ist der wohl lukrativste Bereich der Kriminalität und in der Schweiz stark auf dem Vormarsch. Allein im Jahr 2023 erhielt das Bundesamt für Cybersicherheit (BACS) knapp 50'000 Meldungen zu Cyberkriminalität, ein Anstieg von 30 Prozent im Vergleich zum Vorjahr. Die oft aus dem Ausland agierenden Täter können von den Schweizer Behörden kaum ermittelt werden, weshalb nur wenige Täter tatsächlich zur Rechenschaft gezogen werden. Es liegt daher an den potenziellen Opfern, den Unternehmen und Privatpersonen in der Schweiz, sich gegen diese Bedrohung zu wehren.

In der Praxis hat sich gezeigt, dass die grösste Gefahr, Opfer eines Cyberangriffs zu werden, vom Faktor Mensch ausgeht. Sei es durch Mitarbeitende, Kunden oder durch die eigene Unachtsamkeit. Der vorliegende Spotlight soll auf diese Gefahren aufmerksam machen und aufzeigen, wie dem Risiko Mensch bestmöglich begegnet werden kann: Sie sind den Angriffen krimineller Hacker nicht schutzlos ausgeliefert!

Prävention

Eine erste Gefahrenbewältigung beginnt mit der Sensibilisierung sowie mit entscheidenden Vorbereitungsschritten. Die Etablierung eines sinnvollen Präventionsprogramms ist unumgänglich für eine pragmatische Krisenbewältigung. Für ein gut funktionierendes Präventionsprogramm sind in Bezug auf menschliche Faktoren insbesondere die folgenden Punkte zentral:

- Sensibilisierung: Innerhalb des Unternehmens müssen sämtliche Mitarbeitende periodisch auf die Cybergefahren und das richtige Verhalten hingewiesen werden. Ein Verteidigungsdispositiv ist nur so stark wie das schwächste Glied der Kette. Insbesondere muss ein Bewusstsein und eine Wachsamkeit geschaffen werden für Phishing (das «Fischen» von Login-Daten) und Social-Engineering (Betrugsversuche durch Identitätsmissbrauch). Cyber-Kriminelle können durch Social-Engineering beinahe jeden täuschen – dessen sollten sich alle bewusst sein.

  Eine Massnahme zur direkten Sensibilisierung von Mitarbeitenden kann sein, dass in unregelmässigen Abständen simulierte Phishing-Mails durch die eigene IT versendet und dadurch Schwachstellen (im Sinne von unachtsamen Personen) aufgedeckt werden können.

- Verantwortlichkeiten definieren: Es ist eminent wichtig, zentrale Verantwortlichkeiten im Falle eines Cyber-Angriffs festzulegen. Jedem Mitarbeitenden muss zu jedem Zeitpunkt klar sein, an wen man sich im Falle einer Unklarheit oder im schlimmsten Fall bei einer Cyber-Attacke wenden kann. Dies sollte auch die Information umfassen, dass Mitarbeitende suspekte E-Mails oder externe USB-Sticks an die unternehmensinterne IT oder den externen IT-Dienstleister zur Überprüfung weiterleiten sollen. Auch für Privatpersonen ist es wichtig zu wissen, dass verdächtige E-Mails oder Dateien über gratis verfügbare Webtools (bspw. VirusTotal) geprüft werden können; bei vertraulichen Daten ist dabei Vorsicht geboten.

- Weisung für Cyber-Incidents und Krisenmanagement: Unumgänglich ist es weiter, im Rahmen einer Arbeitgeberweisung die Handhabung von Cyber-Incidents und das Krisenmanagement festzulegen. Diesbezüglich ist insbesondere darauf einzugehen, wie und an wen Cyber-Vorfälle durch die Mitarbeitenden unverzüglich zu melden sind. Die schlimmste Situation ist diejenige, in welcher die Mitarbeitenden den Cyber-Angriff zwar bemerken, aber nicht wissen, an wen und in welcher Form dies intern zu melden ist. Dadurch geht wertvolle Zeit verloren – Zeit, welche die Angreifer zur Schädigung des Opfers nutzen können.

  Auch das Krisenmanagement bedarf einer separaten Regelung. Es ist wichtig, dass Mitarbeitende, welche Cyber-Schwachstellen oder gar Angriffe melden, sich ernst genommen fühlen. Ein entsprechendes Whistleblowing- oder Krisenmanagement-Setup ist unverzichtbar. Ansonsten riskieren betroffene Unternehmen, dass unzufriedene Mitarbeitende lieber mit der Presse oder Dritten sprechen als mit den zuständigen internen Stellen.

- Cyber-Notfallprotokoll: Mit der zusätzlichen Erstellung eines Cyber-Notfallprotokolls für den Fall einer Cyber-Attacke werden etwaige Redundanzen in einer Krisensituation bereits vor dem Eintreten der Attacke effektiv und gewinnbringend beseitigt. In einem solchen Notfallprotokoll sollen insbesondere die notwendigen Schritte zur Sicherstellung der internen und externen Kommunikationswege inkl. Meldepflichten zur Eindämmung einer Cyber-Attacke und für die Wiederaufnahme des operativen Betriebs festgelegt werden. Zudem lohnt es sich, die bereits vorbestehenden Kontakte zu externen Dienstleistern wie IT-Experten, Rechtsberatern oder eine Kommunikationsagentur für allfällige Presseanfragen festzulegen.

- Versicherung gegen Cyber-Angriffe: Mit einer aus Sicht der Täter erfolgreichen Cyber-Attacke sind für Betroffene notwendigerweise Kosten und Aufwand verbunden. Selbst die gelungene Abwehr einer Cyber-Attacke ohne Geld- oder

Datenabfluss bindet Ressourcen und kann teuer werden. Sollte eine Versicherung gegen Cyber-Angriffe abgeschlossen worden sein, bleibt zu beachten, dass die versicherungsvertraglichen Melde- und Schadensminderungspflichten eingehalten werden müssen. Auch aus diesem Grund ist es essenziell, mit der Aufarbeitung des Cyber-Vorfalles umgehend zu beginnen.

Sodann bleibt auch zu prüfen, ob bereits abgeschlossene Versicherungen eventuell auch den Schadenseintritt durch Cyber-Attacken abdecken.

SELBST DIE BESTE PRÄVENTION KANN DIE MÖGLICHKEIT EINES ERFOLGREICHEN CYBER-ANGRIFFS BLOSS MINIMIEREN.

Reaktion

Selbst die beste Prävention kann die Möglichkeit eines erfolgreichen Cyber-Angriffs nicht vollständig beseitigen, sondern dessen Eintrittswahrscheinlichkeit bloss minimieren. Für ein erfolgreiches Cyberkriminalitäts-Abwehrdispositiv ist es deshalb notwendig, dass Betroffene sich bereits das Wissen und die Reaktionsmöglichkeiten für den konkreten Umgang mit einem Cyber-Angriff angeeignet haben. In Bezug auf eine adäquate Reaktion auf einen Cyber-Angriff ist das Nachfolgende zu beachten:

- Hochfahren des Betriebes und Dokumentation: Eine angemessene Reaktion auf einen Cyber-Vorfall beinhaltet selbstverständlich im ersten Schritt, dass der Betrieb bzw. die IT-Systeme so bald als möglich wieder hochgefahren werden. Diesbezüglich muss jedoch besonders darauf geachtet werden, dass bei der Wiederaufnahme des Betriebs keine Beweismittel zur Aufarbeitung der Cyber-Attacke vernichtet werden. Es lohnt sich deshalb, die Auswirkungen des Cyber-Angriffs auf die IT-Systeme und die Aufarbeitung des Angriffs von Beginn weg zu dokumentieren. Dadurch wird gewährleistet, dass eine spätere Untersuchung und Fehleridentifikation möglich ist. Eine verständliche Dokumentation ist zudem auch für die Meldung an die Versicherung notwendig.

- Untersuchung und Fehleridentifikation: Sobald die unmittelbaren Auswirkungen des Cyber-Angriffs beseitigt sind, ist eine Untersuchung des Vorfalls und eine Identifikation der (menschlichen) Fehlerquelle unausweichlich. Durch diese Untersuchung können wertvolle Erkenntnisse gewonnen werden, welche eine Wiederholung eines erfolgreichen Cyber-Angriffes in der Art des Eingetretenen verhindern können. Solche Untersuchungen sind aufwendig und erfordern innerhalb kürzester Zeit grosse Ressourcen. Häufig lohnt es sich für die Aufarbeitung des Cyber-Vorfalles deshalb, mit externen Partnern zusammenzuarbeiten.

  Durch die interne Untersuchung und die Identifikation der Fehlerquelle lässt sich sodann festlegen, ob die vorgehend erlassenen Cyber-Weisungen sowie das Notfallprotokoll eingehalten wurden bzw. ob die Prozesse überhaupt einen ausreichenden Schutz bieten. Dadurch lassen sich im Rahmen einer späteren Strafanzeige zentrale Beweismittel bereits in einem frühen Stadium produzieren. Sodann lassen sich durch diese Aufarbeitung Haftungsrisiken des Managements minimieren. Ebenfalls lässt sich durch diese Aufarbeitung und eine etwaige Fehleridentifikation gegenüber der Versicherung nachweisen, dass kein Selbstverschulden vorliegt, welches die Versicherungsleistung minimieren oder gar ganz ausschliessen würde.

- Meldepflichten: Um die Haftungsrisiken des Unternehmens oder des Managements zu minimieren, ist umgehend zu prüfen, ob Meldepflichten an Behörden oder an Kunden bestehen. Ein Cyber-Vorfall kann unterschiedliche behördliche Meldepflicht auslösen. Stellt ein Vorfall ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen dar, hat umgehend eine Meldung an den eidgenössischen Datenschutzbeauftragen zu erfolgen[1]. Gilt ein Unternehmen als kritische Infrastruktur, was unter anderem für Banken, Versicherungen und gewisse Internetdienstleister zutrifft, hat innerhalb von 24 Stunden nach einer Cyber-Attacke eine Meldung an das BACS zu erfolgen[2]. Im Gegenzug haben die meldepflichtigen Organisationen Anspruch auf Unterstützung durch das BACS bei der Bewältigung des Cybervorfalls. Untersteht das Unternehmen der Regulierung durch die eidgenössische Finanzmarktaufsicht FINMA und handelt es sich um eine Cyber-Attacke von wesentlicher Bedeutung, hat zudem innerhalb von 24 Stunden eine Meldung an die FINMA zu erfolgen[3].

  Ein Cyber-Vorfall kann zudem eine Meldepflicht an einen Kunden oder andere betroffene Personen auslösen. Betroffene Personen müssen in erster Linie dann über einen Vorfall informiert werden, wenn diese durch bestimmte Massnahmen die Risiken für ihre Persönlichkeit oder Grundrechte (noch) reduzieren können, beispielsweise indem sie ihre Kreditkarte sperren nach einer Cyber-Attacke auf ihre Bank.

  Um im Ernstfall die Meldepflichten frist- und pflichtgemäss erfüllen zu können, und damit das Risiko einer zivil- und strafrechtlichen Haftbarkeit zu minimieren, sollten Unternehmen folgende Fragen im Vorfeld beantworten:

  - Welche Art von Cyber-Vorfällen könnte eine Meldepflicht an den Datenschutzbeauftragen auslösen?
  - Untersteht das Unternehmen einer generellen Meldepflicht gegenüber einer Behörde, bspw. gegenüber dem BACS?
  - Welche Informationen haben wir im Ernstfall an welche Behörde zu melden und in welchem Zeitraum?

- Lösegeldzahlung: Die Zahlung von Lösegeld im Falle eines Ransomware-Angriffs stellt für viele Betroffene eine naheliegende Option dar, um schnell wieder Zugriff auf ihre Daten zu erhalten. Erfahrungsberichte zeigen, dass Hacker oft nach der Überweisung des Lösegelds, meist in Kryptowährungen, die versprochenen Zugeständnisse wie die Entsperrung von Servern rasch umsetzen. Das Hacking ist

1 Art. 24 Abs. 1 Datenschutzgesetz
2 Art. 74e Abs. 1 Informationssicherheitsgesetz
3 FINMA-Aufsichtsmitteilung zur Meldepflicht von Cyber-Attacken

ein Geschäftsmodell und Hacker agieren häufig in professionellen Organisationen, die ihre Glaubwürdigkeit wahren wollen. Bei den Verhandlungen haben Opfer daher – wenn auch nur wenig – Verhandlungsspielraum, denn die Angreifer kommen nur zu ihrem Ziel, wenn tatsächlich eine Zahlung erfolgt. Man beachte aber, dass man es hier mit Kriminellen zu tun hat, was eine gewisse Unberechenbarkeit der Gesamtsituation mit sich bringt. Wichtig: Dies alles bedeutet nicht, dass zwingend eine Zahlung zu erfolgen hat. Die Entscheidung, ob eine Lösegeldzahlung erfolgen soll, ist eine Interessenabwägung und eine wirtschaftliche (und allenfalls auch emotionale) Einschätzung der potenziell verloren gehenden Daten. Alternative Lösungen wie etwa die Wiederherstellung aus Backups oder die Zusammenarbeit mit Cyber-Sicherheitsexperten können genauso attraktiv sein und sind mit dem eigenen Rechtsempfinden vermutlich besser vereinbar.

- Strafanzeige: Unabhängig von der Bezahlung eines Lösegeldes sollte umgehend eine Strafanzeige bei den Strafverfolgungsbehörden eingereicht werden. Polizei und Staatsanwaltschaft verfügen häufig über ausreichend technische und spezialisierte personelle Ressourcen, um eine Cyber-Attacke abzuwehren, aufzuarbeiten oder im besten Falle sogar abgezogene Vermögenswerte oder Daten zurückzuholen. Sodann lassen sich durch die Einleitung eines Strafverfahrens Beweismittel sichern, welche für den etwaigen Schadensrapport an die Versicherung hilfreich sind. Diese Beweismittel können auch den Prozess der Fehleridentifikation beschleunigen und dazu beitragen, etwaige Schwachstellen in den Prozessen des Opfers zu verbessern.

Die sich Unternehmen und Privatpersonen stellenden Probleme im Zusammenhang mit Cyber-Sicherheit und der Abwehr von Cyber-Attacken sind vielseitig, anspruchsvoll und keineswegs auf technische Fragen beschränkt. Für ein schlagkräftiges Abwehrdispositiv lohnt es sich deshalb, frühzeitig professionelle Hilfe beizuziehen. Bei den Tätern handelt es sich schliesslich auch um Profis.

Keyfacts

01 Cyberkriminalität kann jeden treffen, daher ist eine frühzeitige Vorbereitung entscheidend.

02 Effektive Prävention erfordert Sensibilisierung der Mitarbeitenden, klare Verantwortlichkeiten und ein Notfallprotokoll.

03 Bei einem Cyber-Vorfall ist rasches, durchdachtes Handeln entscheidend, um den Betrieb rasch wieder aufnehmen und Beweise sichern zu können.

04 Unternehmen sollten ihre Meldepflichten prüfen und allenfalls Kunden informieren, um Haftungsrisiken zu minimieren.

Michael Mráz
Partner
m.mraz@wengervieli.ch
+41 58 958 53 18

Claudia Keller
Partnerin
c.keller@wengervieli.ch
+41 58 958 53 15

Loris Baumgartner
Associate
l.baumgartner@wengervieli.ch
+41 58 958 53 44

Matthias Langenegger
Associate
m.langenegger@wengervieli.ch
+41 58 958 53 43

Wenger Vieli ist Ihr verlässliches Gegenüber in Rechts- und Steuerfragen. Wir sind nicht nur fachlich exzellent, erfahren und verantwortungsbewusst, wir sind auch neugierig! Statt Grenzen sehen wir Möglichkeiten, entwickeln Lösungen und eröffnen Perspektiven. Dies tun wir mit Freude. In der Schweiz, Europa und der restlichen Welt.