Cyberattacke – wie sich schützen

Checkliste für Unternehmensleitung im Falle eines Cyberangriffs

Management Summary

1. Eine gute Strategie gegen Cyberangriffe beginnt vor dem eigentlichen Vorfall:
   Die Unternehmensführung soll sich vorgängig überlegen, wie sie reagieren wird.

2. Kommt es zu einem Cybervorfall, ist schnelles Handeln angezeigt:
   Eingespielte Prozesse und Eskalationspfade helfen sehr, die Kontrolle über die Lage zu behalten.

3. Nach dem Angriff ist vor dem Angriff:
   Eine systematische Nachbearbeitung bei Cyberangriffen ist wesentlich.

1. Vorbereitung

Allgemeine Massnahmen der Geschäftsleitung:
> Gibt es in Ihrem Unternehmen ein Krisenteam für den Fall eines Cyberangriffs? Wurden klare Verantwortungsbereiche und Zuständigkeiten definiert und mit dem Krisenteam trainiert?
> Ist das Krisenteam mit den benötigten Ressourcen und Kompetenzen ausgestattet? (Im Besonderen Unterstützung im Bereich Krisenmanagement, interne und externe Kommunikation, Recht, Personal und technische Experten/-innen)
> Verfügt das Krisenteam über ein aktuelles Handbuch mit relevanten – aktuellen – Kontaktdaten von (den entscheidenden) Vertretenden externer Partner/-innen?
> Unterzieht sich das Team regelmässigen Übungen, sodass die Mitglieder sich gegenseitig und die Rollen und Verantwortlichkeiten innerhalb des Teams genau kennen?
> Ist das Team mit den Prozessen der Strafverfolgung oder der technischen Beratung durch die Polizei / die Ansprechpartner vertraut?
> Gibt es persönliche Verbindungen zwischen Ihrem Unternehmen oder Ihrem Krisenteam und der Strafverfolgung?

Rechtliche Massnahmen:
> Gibt es klar definierte Verantwortlichkeiten in Bezug auf Führung, Kommunikation und Rechtsabteilung, ob und wann es angebracht ist, die Polizei zur Beratung zu kontaktieren oder die Polizei zur Untersuchung aufzufordern?
> Ist den Verantwortlichen die Differenzierung zwischen beratender Polizei und strafverfolgender Polizei klar?[1]

2. Im Schadenfall

> Für den Fall eines privaten Ärgernisses hilft der Weg zum nächsten Polizeiposten.
> Im Falle eines Falles, d.h. bei einem akuten Cyberangriff gegen ein Unternehmen, geht es darum, rasch Spezialisten/-innen aufzusuchen. Kontaktieren Sie umgehend die Polizei. Auf dem Suisse-ePolice-Online-Portal (www.suisse-epolice.ch) finden Sie die Telefonnummer eines Polizeipostens in Ihrer Nähe.
  > Spezialisierte privatwirtschaftliche Unternehmen helfen Ihnen, Ihre Infrastruktur zu reparieren und gegebenenfalls wiederherzustellen.

1 Vergleichen Sie dazu die Ausführungen auf Seite 2.

- Ihre Polizei berät und unterstützt Sie im weiteren Vorgehen, insbesondere auch in der Frage, ob allfälliges Lösegeld bezahlt werden soll.
  Die Polizei ist grundsätzlich weder an Ihren Geschäftsgeheimnissen interessiert noch daran, auf Ihre Infrastruktur einzuwirken. Vielmehr ist die Polizei darauf angewiesen, dass ein angegriffenes Unternehmen von sich aus bereit ist, die von der Täterschaft auf den Systemen der Geschädigten hinterlassenen Spuren herauszugeben.
  Wird ein Unternehmen akut angegriffen, ist es empfehlenswert, sich durch technisch versierte Mitarbeitende direkt mit spezialisierten Mitarbeitenden der Polizei telefonisch in Verbindung zu setzen. Der/die entsprechende Mitarbeitende braucht zwingend die interne Freigabe, typischerweise vom Management, bzw. von «Legal». Das Unternehmen braucht eine entsprechende Policy, auch ob «Legal» den Anruf live mitverfolgt.
- Die Melde- und Analysestelle des Bundes (MELANI) hilft Ihnen, einzuschätzen, von welcher Schadsoftware Sie befallen und ob noch weitere Unternehmen betroffen sind.

3. Nachbereitung

Gibt es eine systematische Nachbereitung von Schadenfällen (oder auch «near misses», bei denen es gerade noch gut gegangen ist) bezüglich der kontinuierlichen Verbesserung?

Potenziell verbessert werden können durch eine Nachbearbeitung insbesondere
- die präventive oder zeitnahe Erkennung eines Vorfalls,
- die Qualität und Geschwindigkeit der Vorfalleinschätzung (Schadenausmass, Kritikalität usw.),
- die angemessene und zeitnahe Reaktion/Eskalation bei Bedarf,
- die Bewältigung des Vorfalls, sowohl bezüglich allfälliger Sofortmassnahmen zur Eindämmung des Schadenausmasses als auch der Identifikation und Behebung der eigentlichen Ursachen und Schwachstellen,
- die Massnahmen und Hilfsmittel zur Aufrechterhaltung eines angemessenen Notbetriebs während der Vorfallbewältigung,
- die Kommunikation nach innen und aussen,
- die Effektivität und Effizienz der organisatorischen und technischen Massnahmen, Hilfsmittel und Abläufe sowie
- die interne Zusammenarbeit sowie die Zusammenarbeit mit externen Instanzen.

Ein aktiver Erfahrungsaustausch bezüglich Vorfallbewältigung mit anderen Instanzen in der gleichen Branche, Region oder Rechtsumgebung ist ein weiteres Instrument zur effektiven Nachbearbeitung. Die erworbenen Erkenntnisse sollen systematisch in die Qualitätsverbesserung, in die internen Prozesse, Dokumentationen, Übungen und in die Unternehmensführung und -kultur eingebunden werden.

In Zusammenarbeit mit MELANI und Swiss Cyber Experts