Im Visier von Cyberattacken

Obwohl die Anzahl Cyberangriffe in der Schweiz stetig steigt, ergreifen viele Unternehmen keine ausreichenden Massnahmen und erachten das Thema als erledigt, sobald IT-Dienstleister mit im Boot sind. Ein Trugschluss, denn für den optimalen Schutz ist nicht nur eine aktive Zusammenarbeit mit Expertinnen und Experten nötig, sondern auch eine klare Rollenverteilung sowie die angemessene Schulung und Information der Mitarbeitenden.

Von Florian Muff
Manager
Forensic Technology & Cyber Security
BDO AG

In vielen Fällen setzen Cyberkriminelle bei ihren Angriffen nicht auf neuste Technologien, sondern nutzen die Trägheit von Unternehmen, Organisationen oder Privatpersonen aus. Der entstandene Schaden ist meist gross – allzu oft wäre er vermeidbar gewesen.

Ein Grossteil der Cyberattacken wird durch Massen-E-Mails oder Massenscans lanciert. Gut geschützte Unternehmen sind dabei nicht nur angriffsresistenter, sondern werden auch weniger oft zum Ziel von Attacken. Umso wichtiger ist es daher, dass sich verantwortliche Personen laufend über aktuelle Gefahren rund um Cyberkriminalität und deren Gestaltungsformen informieren und mit dem Thema aktiv auf IT-Dienstleister zugehen.

Wie es um die Cybersicherheit im eigenen Unternehmen steht, lässt sich anhand der folgenden Fragen ermitteln:

1. Erkennen die Mitarbeitenden einen Cyberangriff, zum Beispiel in der Form einer Phishing-E-Mail?
Phishing-E-Mails sind bei Cyberkriminellen ein beliebter Weg, um sich Zugang zu IT-Systemen zu verschaffen. Sie werden immer raffinierter aufgebaut, und bereits heute verwenden die Täter bei mehr als der Hälfte ihrer Angriffe Informationen über die Rezipienten, um deren Vertrauen zu erlangen. Oft reicht ein falscher Klick und schon ist ein Unternehmen kompromittiert. Phishing-E-Mails und ähnliche Attacken nutzen menschliche Schwächen aus, durch eine effektive Sensibilisierung der Mitarbeitenden kann das Risiko aber deutlich gesenkt werden.

2. Wissen die Mitarbeitenden, was bei einem Angriff zu tun ist?
Ein geschulter Umgang mit der Gefahr und eigenen Fehlern ist von zentraler Bedeutung. Mitarbeitenden muss klar sein, wie sie im Ernstfall vorgehen und an wen sie sich wenden müssen. Im Unternehmen sollte ein Bewusstsein für die Abläufe geschaffen werden, indem Cyberkriminalität und der Umgang damit kontinuierlich thematisiert wird. Empfehlenswert ist es, das Personal mehrmals im Jahr auf aktuelle Trends rund um Cyberkriminalität aufmerksam zu machen.

3. Existiert ein Notfallplan, falls der Computer verschlüsselt wurde?
Zentrale Abläufe werden vielfach über den Computer gesteuert. Ein Ausfall kann dazu führen, dass gewohnte Vorgehensweisen nicht mehr möglich sind. Ein Notfallplan sorgt primär dafür, dass Zuständigkeiten und Abläufe festgelegt sind und diese entsprechend kommuniziert werden. Dadurch kann in einer Angriffssituation direkt adäquat reagiert werden. Da Cyberattacken elektronische Geräte oder Server in vielen Fällen ausser Betrieb setzen, empfiehlt es sich, die Notfallpläne auch in gedruckter Form zur Hand zu haben.

4. Wie sind die Daten gesichert? Gibt es ein Back-up und ist sichergestellt, dass dieses funktioniert?
Um zu vermeiden, dass das Unternehmen den Zugang auf die eigenen Daten verliert und dadurch sowohl erpressbar als auch handlungsunfähig wird, ist das Erstellen von Back-ups im Ernstfall ausschlaggebend. So lässt sich der Schaden von Attacken begrenzen. Mit regelmässigen Tests der Infrastruktur kann sichergestellt werden, dass die Backups zuverlässig durchgeführt werden.

5. Sind die Verantwortlichkeiten bezüglich Sicherheitsmassnahmen klar geregelt?
Eine klare Rollenverteilung ist essenziell, um effiziente Abläufe in der Prävention und Bekämpfung von Angriffen zu gewährleisten. Da es sich vielfach um sehr technische Prozesse handelt, muss jemand die Verantwortung übernehmen, der über das nötige Know-how verfügt. Die Aufgabenteilung muss nicht nur intern, sondern auch extern klar geregelt sein. Zudem muss gewährleistet werden, dass die geplanten Massnahmen effektive Mittel gegen Cyber–attacken darstellen. Auf der Suche nach einem externen Dienstleister bietet eine Orientierung am Gütesiegel «Cyberseal» Unterstützung.

Falls die Mehrzahl der oben genannten Fragen mit «Nein» beantwortet wurde, gilt es, Schritte einzuleiten und bestehende Sicherheitslücken zu schliessen. Unabhängig vom Ergebnis der Fragen ist ein Test des derzeitigen Sicherheitsniveaus immer eine gute Idee.

cybersecurity@bdo.ch
www.bdo.ch