„Sind wir sicher?"

"Sind wir sicher?" - eine Frage, welche viele CISOs regelmässig hören und viele Geschäftsleitungsmitglieder regelmässig stellen. Speziell in Zeiten, in denen regelmässig über Kryptotroyaner, Attacken gegen Schweizer Firmen, in denen Millionen von Schweizer Franken entwendet werden und Industriespionage in den Medien berichtet wird, beschäftigt sich die Geschäftsleitungsebene mit dieser Frage. Zu Recht. "Sind wir sicher?" - Eine simple Frage. Doch die Antwort darauf treibt vielen CISOs den Schweiss auf die Stirn. Denn so simpel die Frage ist, so schwierig ist sie auch zu beantworten. Das liegt jedoch nicht an der fehlenden Fachkompetenz des CISOs, sondern an der Entwicklung der Cyber-Bedrohungen, der Komplexität der heutigen IT-Landschaft und der Sichtweise, auf welcher diese Frage basiert.

Cyber-Bedrohungen nehmen stetig zu. Cyber-Kriminalität hat sich in den letzten Jahren zu einem grösseren Wirtschaftszweig entwickelt als der globale Drogenhandel. Hacker sind nicht mehr schlecht gekleidete, schlecht ernährte Personen, welche zu wenig Sonnenlicht erhalten. Es sind Personen, welche in einer Unternehmung angestellt sind, geregelte Arbeitszeiten haben und während dieser Arbeitszeit andere Unternehmen hacken. Vielfach kann man an den Zeitcodes eines Angriffes einfach erkennen, von wo der Angriff ausgeführt wird. Zusätzlich kann Malware heute im Internet mit einem SLA und einer Hotline-Nummer gekauft werden - mit Garantieleistungen, falls die Malware von einem Antivirus Produkt identifiziert wird. Somit ist es nicht mehr notwendig umfassende technische Kenntnisse zu besitzen, um einen Malware-Angriff zu starten. Denial of Service Attacken können für wenige US Dollar gekauft werden. In einem Menu lassen sich das Protokoll, die Bandbreite und die Dauer einfach auswählen. Cyber-Attacken werden zur Commodity, welche jedermann ohne grosses Vorwissen bestellen kann. Die Konsequenz aus diesen Entwicklungen ist, dass wir nicht mehr wissen, wer uns wann mit welchen Mitteln angreifen wird.

Auch die **Komplexität** und die Abhängigkeit von Unternehmen von ihrer IT-Landschaft nimmt zu. Immer mehr Business Services hängen immer stärker von einer funktionierenden, intakten IT-Landschaft ab. Auch scheinbar simple Prozesse können heute nicht mehr funktionieren, wenn die darunterliegende IT nicht funktioniert. Zudem stellen Mitarbeitende immer grössere Ansprüche an ihren Arbeitgeber. Gratis WiFi, um diverse private Geräte mit dem Internet zu verknüpfen, Bring Your Own Device, damit jeder Mitarbeitende seine Arbeit auf einem von ihm/ihr selbst ausgewählten Modell ausführen kann, Single-Sign-On, damit das lästige Passwort nicht andauernd eingegeben werden muss – dies sind nur einige Beispiele von Entwicklungen, welche für Unternehmen zu kostspieligen Herausforderungen werden, die die Komplexität ihrer IT-Landschaft massiv erhöhen. Viele IT-Teams haben kaum mehr einen Überblick über die wahren Abhängigkeiten in ihrer Landschaft. Der Ausfall eines Systems hat oft unerwartete Konsequenzen an unerwarteten Orten. Und der CISO hat die Aufgabe, hier eine Übersicht zu haben und die Security zu gewährleisten.

Das Schwierigste an der Frage "Sind wir sicher?" liegt jedoch in der **Sichtweise**, auf welcher diese Frage beruht. Wir wissen erst, dass wir sicher sind, wenn wir wissen, welches die Bedrohungen sind und wie unsere IT-Landschaft auf diese Bedrohungen reagieren wird. Wir haben jedoch festgestellt, dass wir gar nicht wissen, wer uns wann wie angreifen wird. Auch basiert diese Frage auf einer "Wenn-Dann-Sichtweise": Wenn wir angegriffen würden, wären wir dann sicher? Jede Unternehmung wird dauernd angegriffen - von verschiedensten Gruppen mit verschiedensten Mitteln. Somit kann man nicht mehr von einer Angriffswahrscheinlichkeit sprechen - sie läge nämlich bei 100%. Sobald wir akzeptieren, dass unsere Unternehmung angegriffen wird, ändert sich automatisch auch unsere Sicht auf Informationssicherheit. Es geht dann plötzlich nicht mehr nur darum, uns gegen Attacken zu schützen, sondern auch darum, Attacken zu entdecken und richtig und schnell darauf zu reagieren.

Dies ist der Ansatz von **Cyber Resilienz**. Resilienz ist die Fähigkeit eines Systems, trotz externer negativer Einflüsse einen akzeptablen Service Level zu halten. Unternehmen müssen den Glauben abgeben, dass man sich gegen alle Bedrohungen schützen kann. Wir müssen akzeptieren, dass wir angegriffen werden, aber trotzdem unsere IT-Systeme betreiben können. Um dies tun zu können, brauchen wir eine Kombination von Schutz-, Detektions- und Reaktionsmassnahmen. Die Schutzmassnahmen schützen vor Bedrohungen, welche bekannt sind. Detektionsmassnahmen informieren über Aktivitäten, gegen welche die Schutzmassnahmen nutzlos waren und deren Qualität bestimmt, wie schnell die Aufräumarbeiten beginnen können. Die Reaktionsmassnahmen sorgen dafür, dass die betroffenen IT-Services so schnell wie möglich in einen akzeptablen Service Level zurückkehren können und die Bedrohung effizient und effektiv bereinigt wird.

Zurück zur Frage "Sind wir sicher?". Nun, eigentlich ist die Frage falsch gestellt, da sie das Thema Informationssicherheit aus einem falschen Blickwinkel heraus betrachtet. Dies ist auch einer der Gründe, weshalb CISOs es oft sehr schwierig finden, auf diese Frage eine gute Antwort zu geben. Wenn jedoch die Frage geändert wird in "Sind wir widerstandsfähig genug?", wird einerseits wirklich das gefragt, was die Geschäftsleitung erfahren möchte und andererseits können CISOs, wenn sie mit den richtigen Mitteln ausgestattet sind, eine sehr übersichtliche und einfach verständliche Antwort darauf geben.

Autor:
Craig Fletcher
Chief Consulting Officer
craig.fletcher@ispin.ch