Tabletop-Übung

Vorbereiten auf den Cybervorfall

Die Frage ist nicht ob, sondern wann: Wer für den Ernstfall «Cyberangriff» nicht nur einen Plan in der Schublade ablegt, sondern diesen auch durchgespielt und geübt hat, wird im Notfall einen kühlen Kopf bewahren und gut durch die Krise kommen.

→ VON CHRISTIAN FICHERA

DER AUTOR

Christian Fichera
ist Senior Cyber Security Consultant bei terreActive und Leiter des Teams Audit, Risk & Compliance. Seine Abteilung verfügt über langjähriges Security-Know-how, das unter anderem auf Projekten zu Penetrationstests, Red-Team-Services und Secure Code Review für Unternehmen verschiedener Branchen in der Schweiz basiert.
→ www.security.ch

Jedes Unternehmen kann früher oder später von einem Katastrophenszenario wie einem Cybervorfall betroffen sein. Neuste Zahlen des Sicherheitsanbieters Check Point zeigen, dass Schweizer Firmen in den letzten 10 Monaten durchschnittlich 675 Mal pro Woche (!) angegriffen wurden. Es ist also unabdingbar, dass man sich auf den Worst Case vorbereitet.

WAS IST EINE TABLETOP-ÜBUNG?

«Tabletop» bezeichnet eine Übung auf dem «Tisch», ohne Einsatz von IT-Komponenten, also ausschliesslich auf Basis dokumentierter Informationen, wie beispielsweise Reglemente, Checklisten, Notfall-Prozesse, um nur einige zu nennen. In einem Rollenspiel wird das Szenario eines Cybervorfalls durchgespielt und die Reaktionsfähigkeit des Unternehmens bewertet.

In der Regel führt ein externer Security-Spezialist die Übung ganztägig vor Ort beim Kunden durch. Beteiligt sind Personen aus verschiedenen Organisationseinheiten, die auch bei einem echten Vorfall involviert wären. Abhängig vom gewählten Szenario haben die Stakeholder einen technischen oder fachlichen Hintergrund, beispielsweise Vertreter der Kommunikationsabteilung, des Krisenstabs (Management) oder der IT-Organisation.

ZIEL UND NUTZEN: CYBER DEFENSE STÄRKEN

Die Übung hilft, die Resilienz-Fähigkeiten des Unternehmens zu verbessern, indem das Bewusstsein für aktuelle Risiken geschärft wird, Abläufe durchgespielt und Schwachstellen in den Prozessen identifiziert werden, um diese nach der Übung zu beheben. So kann die Cyber Defense eines Unternehmens nachhaltig verbessert und gestärkt werden. Gleichzeitig werden alle Beteiligten hinsichtlich Relevanz des Themas sensibilisiert.

ABLAUF

Der Anbieter einer solchen Tabletop-Übung, ein auf Cyber Security spezialisiertes Unternehmen, übernimmt die Rolle der Spielleitung und schildert das vorgefertigte Szenario, beispielsweise, weil hochaktuell, einen Ransomware-Angriff. Der Spielleiter stellt Fragen zur Situation und zum Vorgehen des Kunden. Die Teilnehmer übernehmen jeweils eine Rolle und einen Verantwortungsbereich und reagieren mit unternehmensspezifischen Lösungen und Vorschlägen auf das Ereignis.

Es gibt kein Richtig oder Falsch, der Security-Anbieter beobachtet und notiert nur. Argumentieren ist erwünscht, da Probleme oder Unklarheiten am besten sofort gelöst werden. Insbesondere wird darauf geachtet, ob etwas fehlt, wo Optimierungen möglich sind und wie auf kurzfristige Veränderungen unter Berücksichtigung des Stressfaktors reagiert wird.

Wichtig ist, dass immer jemand aus dem Security Operations Center verfügbar ist, sei es aus dem eigenen SOC des Kunden oder von dem externen Dienstleister, von welchem SOC-Services bezogen werden. So erleben die Akteure zwar ein fiktives, aber äusserts realistisches Szenario, interagieren miteinander, suchen nach Lösungen und lernen aus Fehlern. Je wirklichkeitsnaher das Szenario, desto besser werden die Teilnehmer auf den Ernstfall vorbereitet. Ein realistisches Customizing erfordert schon in der Vorbereitungsphase eine enge Zusammenarbeit zwischen dem Kunden und dem Spielleiter.

Auf Wunsch des Kunden führt der Spielleiter während der Tabletop-Übung ein Protokoll und übergibt anschliessend einen Bericht mit Erkenntnissen sowie Empfehlungen. Die Übung dauert von einigen Stunden bis zu einem ganzen Tag. Dabei werden die individuellen Anforderungen und Möglichkeiten des Kunden berücksichtigt.

Bild: istockphoto/Hispanolistic

WAS SIND DIE VORTEILE EINER TABLETOP-ÜBUNG?

Unternehmen, die sich für den Probelauf eines Krisenfalles entschieden, taten dies meist aus den folgenden Gründen:

- Lücken und Mängel werden erkannt, Schwachstellen in der Reaktionsfähigkeit bewusst gemacht
- Übung bringt Routine und damit weniger Stress im Ernstfall
- Rollen, Verantwortlichkeiten und Aufgaben innerhalb der Organisation werden geklärt
- Ein Reaktionsplan oder ein «Runbook» werden durchgearbeitet und dabei Dokumente, Prozesse und Kommunikationswege überprüft auf:
  - Verfügbarkeit von Informationen
  - Vollständigkeit
  - Verständlichkeit und Interpretationsspielraum
  - Anwendbarkeit

Bei allen Vorteilen, die eine Tabletop-Übung mit sich bringt, ist es für die IT oder einen CISO auch wichtig, die Abgrenzung zu verstehen: Es handelt sich um eine konzeptionelle Übung – und nicht um ein technisches Audit.

TABLETOP AUS SICHT DES INCIDENT RESPONSE CENTERS

Bei einem Ransomware-Angriff muss das Incident Response Center zuerst reagieren. Eine Tabletop-Übung hilft dem IRC-Team folgende Fragen zu beantworten:

- Wie stellen wir sicher, dass kritische Systeme, Applikationen, Dateien, Datenbanken und andere Ressourcen geschützt sind?
- Wie stellen wir sicher, dass die Ransomware-Attacke im Keim erstickt wird und sich nicht ausbreiten kann?
- Welche Systeme sind für das Unternehmen unverzichtbar und daher besonders schützenswert?

TABLETOP AUS SICHT DES KRISENMANAGEMENTS

Im Falle einer Cyberattacke ist nicht nur das Incident-Response-Team betroffen, sondern auch Vertreter anderer Organisationseinheiten. Diese beschäftigen sich mit folgenden Fragen:

- Sind die Arbeitsmethoden, Prozesse und Verantwortlichkeiten des Notfallplans für alle klar und umsetzbar? Sind die Eskalationswege und Schnittstellen bekannt?
- Funktioniert die Kommunikation und sind die dafür notwendigen Daten vorhanden (ausgedruckte Informationsblätter, Ansprechpartner, Kommunikationsmittel, Aktivitätenprotokoll etc.)?
- Können wichtige Entscheidungen mit den vorhandenen Informationen überhaupt getroffen werden?

AN WEN RICHTET SICH DAS ANGEBOT?

Das Angebot richtet sich an Unternehmen, die bereits über eine IT-Sicherheitsstruktur und über Prozesse für das Krisenmanagement verfügen. Voraussetzung dafür ist, dass das Unternehmen eine IT-Notfallorganisation etabliert hat, oder es muss ein internes bzw. externes SOC vorhanden sein. Sollten die genannten Punkte (noch) nicht erfüllt sein, aber das Unternehmen möchte trotzdem seine Cyber Security verbessern, empfiehlt es sich, mit einem «Readiness-Audit» zu starten. Dabei kann z. B. in einem ersten Schritt überprüft werden, ob der empfohlene IKT-Minimalstandard des Bundesamts für Wirtschaftliche Landesversorgung (BWL) erfüllt wird.

Als Fazit der Tabletop-Übung lässt sich festhalten: Agieren ist immer besser als Reagieren! ←

Das Üben mit realistischen Szenarien hilft, sich auf den Ernstfall vorzubereiten.