Trainings als Vorbereitung für Sicherheitsvorfälle

Gut geübt

Marcel Knop

Wird ein Unternehmen angegriffen oder entdeckt einen Sicherheitsvorfall, ist es häufig überfordert – zumal unter zeitlichem Druck. Durch gezielte Übungen lassen sich solche Situationen besser und schneller bewältigen.

iX-TRACT

- Mit Cyberangriffen ist es wie mit anderen Katastrophen: Nur wenn man gut darauf vorbereitet ist, kann man sie schnell erkennen und effizient damit umgehen.
- Während sich in manchen Bereichen die Fortbildung in Form von Wissensvermittlung bewährt hat, kommt man bei Cyberangriffen damit nicht sehr weit: Hier heißt es üben, üben, üben.
- Das sogenannte Arena-Training, bei dem verschiedene Teams gegeneinander antreten, hat einen weiteren Vorteil. Die Beteiligten erfahren, was in anderen Bereichen vor sich geht, was wiederum das Verständnis füreinander und die Zusammenarbeit fördert.

Das Callcenter wird plötzlich von Anrufen überhäuft, eine große Anzahl verärgerter Kunden beschwert sich über den Ausfall eines wichtigen Dienstes und verlangt Auskunft über Umfang und Dauer der Unterbrechung. IT-Mitarbeiter erkennen vereinzelte Symptome von Störungen, ohne aber die wirkliche Ursache erklären zu können. Erste Social-Media-Postings berichten über die Störung und geben Hinweise, wie eigene Dienste geschützt oder der Dienst trotzdem weiter genutzt werden kann. Die Unternehmenskommunikation, die IT-Abteilung und weitere Fachbereiche beginnen mit Maßnahmen zur Eindämmung und Bewältigung des Vorfalls, leider oft unabhängig voneinander.

Ein vollständiges Bild von der Lage ist nicht vorhanden. Die Unternehmenskommunikation beantwortet Presseanfragen aufgrund der mangelhaften Informationslage nicht oder nur unzureichend. Abteilungen schieben Zuständigkeiten zur Bewältigung des Vorfalls hin und her. Stakeholder erhalten unterschiedliche Auskünfte – oder auch gar keine. Wiederaufnahmeplanen werden falsch priorisiert oder enthalten einige (meist datenschutzrechtliche) Nebenwirkungen, und nicht selten versagen sie gleich ganz ihren erhofften Dienst. Lücken in der Alarmierungs- und Eskalationskette lassen dringende Vorgänge in Vergessenheit geraten. Alle Beteiligten stehen unter hohem psychischem Stress, der wiederum zu einer Vielzahl handwerklicher Fehler führt.

Die Geschwindigkeit und Komplexität eines Cybervorfalls und der Stress der Mitarbeiter überfordern betroffene Unternehmen regelmäßig, wie die Medien immer wieder berichten. Monetäre Verluste durch Produktionsausfall und DSGVO-Bußgelder sowie negative Reputation sind häufig die Folge – oft mit dem Verlust der Deutungshoheit in der Krise einhergehend. Und das, obwohl geeignete Software beschafft und Prozesse zur Vorfallserkennung und -bewältigung eingeführt wurden.

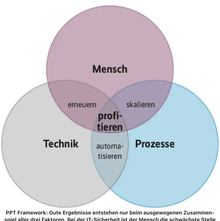
Was kann getan werden, um diese Situationen zu vermeiden?

Wissen, warum: Ursachen analysieren

Reviews derartiger Vorgänge offenbaren ein Muster: Fast immer sind menschliche Fehler die Ursache für Mängel und Verzögerungen im Erkennen und Bewältigen von Vorfällen. Da qualifizierte Angriffe, trotz aller Berichte in den Medien, vergleichsweise selten stattfinden, kommen auch die zur Bekämpfung eingesetzten Tools und die größtenteils manuellen Prozesse selten zur Anwendung – dann aber unter hohem Zeitdruck und Stress.

Demgegenüber sind Polizei, Feuerwehr und Militär häufig mit ähnlichen Situationen konfrontiert – hoher Handlungsdruck bei ungenauer und sich dynamisch entwickelnder Lage. Um diesen Anforderungen zu genügen, hat sich in diesen Bereichen ein umfangreiches Trainingswesen etabliert.

Fähigkeiten entstehen aus dem koordinierten Zusammenspiel von Prozessen, Technik und den beteiligten Menschen. „People – Processes – Technology" (auch PPT Framework) ist ein in diesem Zusammenhang häufig genanntes Beziehungsgefüge. Und tatsächlich, der Reifegrad in den Bereichen „Processes" und „Technology" hat sich in den letzten Jahren deutlich verbessert. Für den Bereich „People" werden meist pauschale Security-Awareness-Schulungen für sämtliche Mitarbeiter angeboten. Zudem existiert eine Vielzahl von Fortbildungen, in denen neues Wissen vermittelt wird. Aber warum bereitet das Erkennen und Beheben von Cybervorfällen dann so häufig große Probleme?



PPT Framework: Gute Ergebnisse entstehen nur beim ausgewogenen Zusammenspiel aller drei Faktoren. Bei der IT-Sicherheit ist der Mensch die schwächste Stelle (Abb. 1).

Quelle: Christopher S. Penn

Fortbildung versus Training

Je nachdem, ob Sachverhalte komplex oder kompliziert sind, unterscheiden sich die Methoden, wie man lernt, mit ihnen umzugehen. Es ist es wichtig, den Unterschied zwischen den beiden Aufgabenstellungen zu kennen:

- In einem komplizierten System gibt es eindeutig definierte Verbindungen der einzelnen Elemente. Auch wenn es ein sehr großes System ist: Alle Zusammenhänge darin sind kausal, folgen also dem Ursache-Wirkung-Prinzip und können vorhergesagt werden. Beispiele sind die Thermodynamik oder das TCP/IP-Referenzmodell. Methode zur Aneignung der Beherrschbarkeit: Lernen.
- Ein komplexes System ist lebendig und seine Ursache-Wirkung-Zusammenhänge sind unüberschaubar. Komplexe Systeme nehmen durch Offenheit zu ihrem Umfeld Informationen auf und entwickeln sich daran angelehnt autonom weiter. Beispiele: Schachpartie, Fußball – oder eben die Reaktion auf schwerwiegende Cybervorfälle. Methode zur Aneignung der Beherrschbarkeit: Trainieren.

Im Fortbildungen wird neues Wissen vermittelt, während in Trainings bereits bekanntes Wissen praktisch angewendet wird. Fortbildungen eignen sich gut für komplizierte Zusammenhänge, weil Wissen zur Erledigung derartiger Aufgaben gut geeignet ist. Trainings sind dagegen für die Bewältigung komplexer Zusammenhänge geeignet, weil hier vor allem Erfahrung gefragt ist.

So gut wie alle Maßnahmen zum Fähigkeitserwerb in Unternehmen basieren auf Fortbildungen. Trainings sind oft nicht etabliert, mit Ausnahme regelmäßig stattfindender Feuerübungen, die die meisten schon seit ihrer Schulzeit kennen dürften. Hierin dürfte auch der Grund liegen, warum Mitarbeiter bei Cybervorfällen häufig schlecht vorbereitet sind – es wurde zu wenig geübt.

Methodik der Angreifer

Der Rüstungskonzern Lockheed Martin hat mit der Cyber Kill Chain die Vorgehensweise bei Cyberangriffen systematisiert und damit ein Beschreibungsmodell für solche Angriffe etabliert. Die in Abbildung 2 dargestellten sieben Phasen müssen erfolgreich durchlaufen werden, um einen Angriff durchzuführen.

Die Cyber Kill Chain beschreibt die einzelnen Phasen, die ein erfolgreicher Angriff durchläuft (Abb. 2).

Um die Cyber Kill Chain aufzudecken und unterbrechen zu können, haben sich Arena-basierte Red-Blue-White-Team-Trainings als realistisches Verfahren bewährt, alle wichtigen Anforderungen des Erkennens und Bewältigens von Cybervorfällen einzuüben.

- Eine Arena ist eine simulierte Umgebung von Schlüsselelementen einer Unternehmens-IT.
- Das Red Team besteht aus (firmeninternen oder dafür engagierten) Angreifern, die über eine Vielzahl von Angriffsmethoden versuchen, in die simulierte Umgebung einzubrechen, ihren Zugriff zu verankern und bestimmte Zielsysteme zu manipulieren. Die Angriffe basieren auf Drehbüchern, die die Cyber Kill Chain abbilden.
- Das Blue Team besteht aus den Verteidigern der simulierten Umgebung, also aus Mitarbeitern des Unternehmens aus den Bereichen SIEM/SOC (Security Information and Event Management/Security Operations Center), Incident Response, IT-Forensikern und dem Unternehmens-Management.
- Das White Team überwacht die Trainingsdurchführung, um sicherzustellen, dass alle im Drehbuch gesteckten Lernziele erreicht werden.

Dem Blue Team bietet sich hiermit eine Möglichkeit, die eigenen Verteidigungsverfahren auf ihre Wirksamkeit zu testen und auch neue Ansätze auszuprobieren – ohne den Ausfall von Produktivsystemen zu riskieren. Während eines Trainings reagiert das Red Team auf die Maßnahmen des Blue Teams und versucht mit Täuschungs- und Ablenkungsmanövern, deren Wirksamkeit zu beeinträchtigen.

Das Set-up einer Trainingsarena besteht neben der abgegrenzten IT-Umgebung aus dem Angreifer-, dem Verteidigungs- und einem Koordinierungsteam (Abb. 3).

Trainings sollten in regelmäßigen Abständen wiederholt werden, um das Gelernte dauerhaft zu sichern. Dabei werden die Angriffe des Red Teams zunehmend komplexer, um einen stetigen Zugewinn der Blue-Team-Fähigkeiten zu ermöglichen (siehe auch Artikel „Das neue Rot" auf Seite 74).

Die Erfahrung hat gezeigt, dass Blue Teams von Unternehmen meist einfache Angriffe erkennen und abwehren können. Mit zunehmender Professionalität der Angriffe sinkt jedoch die Fähigkeit, sie zu erkennen und abzuwehren. Was umso mehr zeigt, wie wichtig derartige Trainings sind, um im Ernstfall schwerwiegende Schäden vom Unternehmen abzuwenden.

Interdisziplinäre Kooperation

Ein interessanter Nebeneffekt eines jeden Trainings ist, dass der fachbereichsübergreifende Austausch zwischen Mitarbeitern eines Unternehmens verbessert wird. Vorbehalte oder Unkenntnis der Arbeitssituation von Produktionsmitarbeitern, IT-Mitarbeitern, Verwaltungs- und Fachmitarbeitern sowie der Unternehmensleitung sind häufig die Ursache für Verzögerungen bei der Bewältigung von Cybervorfällen.

Durch die Trainingssituation und die Moderation durch das White Team entsteht jedoch eine Vielzahl von Möglichkeiten zum persönlichen fachbereichsübergreifenden Austausch unter den Blue-Team-Mitarbeitern.

Neue Perspektiven – neue Erkenntnisse

In vielen Trainings hat sich beispielsweise gezeigt, dass Mitarbeiter eines Security Operations Center durch Teilnahme an einem Krisenstabstraining einen viel genaueren Einduck von den Anforderungen der Krisenstabsarbeit des Unternehmensmanagements erhalten. Umgekehrt ist es für Leitungsmitarbeiter genauso interessant, einen Einblick in die technischen Zusammenhänge eines SOC zu erhalten. Diese Liste ließe sich fortführen.

Der Abbau persönlicher oder fachlicher Hindernisse bei der bereichsübergreifenden Zusammenarbeit ist ein wesentlicher Faktor bei der immer konkreter werdenden Digitalisierung unserer Wirtschaft. Ein gemeinsam durchgeführtes Arena-Training bietet damit eine Vielzahl von Anknüpfungspunkten unter den verschiedenen Mitarbeitergruppen.

Etablierte Verfahren zum Überprüfen der Cybersicherheit sind Penetrationstests, Schwachstellenscans und Audits von Betriebsprozessen und Systemkonfigurationen. Alle diese Formen haben ihre Berechtigung, haben aber unterschiedliche Zielsetzungen und Erkenntnisse.

Während Penetrationstests Sicherheitslücken in einzelnen Systemen aufdecken können, sind Arena-basierte Trainings dazu geeignet, die Dynamik eines Angriffs zu simulieren und die Detektions- und Bewältigungsprozesse des Unternehmens auf ihre quasi vollständige Wirksamkeit zu testen, um sie im Nachgang gezielt zu verbessern.

Diese Vollständigkeit kann auch durch ein Audit der entsprechenden Prozesse nicht erreicht werden, da wesentliche Elemente nur „auf dem Papier" auf ihre Wirksamkeit untersucht werden können.

Fazit und Ausblick

So gut wie jede Innovation enthält mittlerweile eine Cyberkomponente und es ist davon auszugehen, dass dieser Begriff bald verschwinden wird, da jedes Element unseres täglichen Lebens, einschließlich aller Wertschöpfungskomponenten von Unternehmen, einen Cyberanteil enthalten wird. Trotzdem stehen wir noch immer am Anfang der Digitalisierung. Cybervorfälle werden noch häufiger vorkommen und vor allem deutlich schwerwiegendere Folgen haben.

Umso wichtiger wird der gekonnte Einsatz des wahrscheinlich wichtigsten Elements einer jeden Cybersecurity-strategie: für diese Aufgaben vorbereitete und trainierte Mitarbeiter. (uri@ix.de)

Marcel Knop
ist freischaffender Security Consultant und Experte für Audits, Cybertrainings sowie Cyberkrisenmanagement.

Kommentieren