Der Feind aus dem Inneren – wenn Beschäftigte mit Absicht oder aus Versehen Cyberunfälle verursachen

Von Sophos Sicherheitsexperte Michael Veit

Die Cyber-Bedrohungslage für Unternehmen ist vielfältig. Und genau das macht es so schwer, an allen Fronten optimal zu reagieren. Denn es sind längst nicht mehr nur ins Netzwerk geschickte Schadprogramme, die Organisationen das Leben schwer machen. Der menschliche Faktor ist das größte Risiko für jede Organisation, ob wie aktuell im Active Adversary Report als externer Gegner oder als Bedrohung aus dem Inneren.

Es sind in der Regel Mitarbeitende, die auf Phishing-E-Mails klicken, versehentlich von außen kommende E-Mails an alle weiterleiten, Datenträger, Firmenhandys oder Laptops in der Bahn vergessen. Oft werden auch Anwendungen falsch konfiguriert oder nicht korrekt gewartet. Hierdurch vergrößert sich die Angriffsfläche und es besteht die Möglichkeit, dass etwas schief geht. All dies sind wissentliche oder versehentliche Missachtungen interner Geschäftsregeln. Im schlimmsten Fall wird hier gegen Vorschriften von Aufsichtsbehörden verstoßen, was dazu führen könnte, dass das Unternehmen eine obligatorische Offenlegung eines Datenverstoßes und aller damit verbundenen Maßnahmen vornehmen muss.

Positive Fehlerkultur und Aufklärung der Belegschaft
Für Unternehmen ist es eine wichtig, ein Gleichgewicht zwischen Schulung der Mitarbeitenden und Entwicklung einer positiven Einstellung und Kultur in Bezug auf die Widerstandsfähigkeit gegenüber Cyberbedrohungen herzustellen. Dazu gehört die Implementierung klar definierter Prozesse, um diese Kultur zu erhalten sowie die Auswahl derjenigen Technologien, die am besten zu den Mitarbeitenden und Prozessen passen, um Bedrohungen abzuschwächen und Risiken zu minimieren.

Der erste Schritt dazu muss die klare Trennung zwischen dem Privat- und dem Arbeitsleben der Belegschaft sein. Das heißt, Beschäftigten zugewiesene Firmengeräte sind genau das: Firmengeräte. Für persönliche Aktivitäten sollten Privatgeräte genutzt werden.

Für die Akzeptanz und Mitarbeit der Angestellten ist es unerlässlich, sie über ihren privilegierten Zugang zu Werkzeugen und Plattformen aufzuklären, die ihnen bei der Erfüllung ihrer Aufgaben helfen.
Als best practice hat sich die offene Kommunikation über Erwartungen an den Umgang mit internen Informationen bewährt. Die Sensibilisierung in Bezug auf schützenswerte Daten sollte sich zu einer selbstverständlichen Kultur entwickeln.

Gesunde Fehlerkultur müssen alle mittragen
Wie aber können Unternehmen ein Umfeld generieren, in dem sich Beschäftigte ermutigt fühlen, verdächtige Aktivitäten zu melden? Die Aufklärung und der Aufbau einer positiven Unternehmenskultur sind ein entscheidender Faktor, um die Cyber- Resilienz zu fördern.
Hierbei gilt (unerschütterlich) die Einstellung, dass jedes Ereignis eine Lernmöglichkeit ist. Hier gibt es kein falsch oder lächerlich – nur so kann jede und jeder Einzelne lernen, was man besser machen kann. Zudem lassen sich so die abteilungsübergreifende Zusammenarbeit fördern und Korrekturmaßnahmen anstoßen.

Und auch hier gilt: jede Organisation ist nur so stark wie ihr schwächstes Glied. Wenn IT-Verantwortliche einen Prozess zum Aufbau einer starken und gesunden Kultur zur

Minimierung von Insider-Bedrohungen eingeleitet haben, aber nicht die Unterstützung der Geschäftsleitung, des Vorstands oder auch nur einer einzelnen Abteilung erhalten, führt dies zu einem uneinheitlichen Geschäftsgebaren und fördert eine Situation, in der sich ein Risiko zu einem Sicherheitsereignis manifestiert.

Die Schäden für Unternehmen durch Insider-Bedrohungen sind immens
Datenlecks und Datenverluste sind häufig auf Insider-Bedrohungen zurückzuführen, bei denen Informationen, die für das Unternehmen sensibel sind, unkontrolliert versendet werden . Obwohl diese Informationen innerhalb des Geschäftskontextes normalerweise als vertraulich eingestuft würden, werden sie nun „öffentlich" in dem Sinne, dass nicht validierte Personen diese Informationen lesen können.

Die Datenvernichtung ist auch eine sehr typische Aktion, bei der dem Unternehmen die Integrität und Verfügbarkeit von Informationen entzogen wird, so dass es keinen Zugang mehr zu wichtigen Informationen hat – was sich direkt auf die Betriebsfähigkeit des Unternehmens auswirken kann. Datenvernichtung wird häufig mit Ransomware-Betreibern in Verbindung gebracht, ist aber gelegentlich auch auf Insider zurückzuführen. Die Moral von der Geschicht' ist, dass ein bösartiger Insider nicht nur sensible Informationen zur persönlichen Bereicherung stehlen kann, sondern diese auch zerstören oder dem Unternehmen vollständig entziehen kann, um ein Lösegeld für die Rückgabe der Daten zu erpressen.

Was können Unternehmen gegen Insider Bedrohungen machen?
Insider-Bedrohungen lassen sich nur schwer vorhersehen und kontrollieren. Daher ist die Vorbereitung auf die Auswirkungen, die ein Insider verursachen könnte, einer der wichtigsten Prozesse, die es zu bewältigen gilt. Die **Schulung von Mitarbeitenden** in der korrekten Nutzung von Geschäftssystemen und dem Verständnis von Geschäftsprozessen kann viel dazu beitragen, Fehler im Zusammenhang mit versehentlichem Datenabfluss und Datenlecks zu vermeiden. Die **Implementierung technischer Kontrollen**, die den Zugang zu Daten und Systemen regeln, in denen sich sensible Informationen befinden, ist ebenso wichtig wie die **Überwachung der Ergebnisse** dieser Kontrollen und die Reaktion auf Richtlinienverstöße, die ein Anzeichen für schädliche Aktivitäten sein könnten. Sorgen Sie dafür, dass die Mitarbeitenden mit ihrer Arbeit zufrieden sind, und geben Sie ihnen die nötige Unterstützung durch die Geschäftsleitung, damit sie ihre Fähigkeiten bestmöglich einsetzen können.

Interne Bedrohungsszenarien müssen auf die Sicherheitsagenda von Unternehmen
Externe und Insider-Bedrohungen müssen als potenzielles Risiko für ein Unternehmen gleichbehandelt werden. Insider-Bedrohungen müssen in Planungssitzungen für die Reaktion auf Zwischenfälle einbezogen werde. Nicht jeder Insider wird zur Bedrohung, aber er hat zumindest das Potenzial dazu.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de