Cyberattacke – was tun?
Checkliste für CISOs für den Fall eines Cyberangriffs

Technische Massnahmen

> Stellen Sie sicher, dass die Systemzeit Ihrer Netzwerksegmente synchronisiert ist, um ein einfaches Abgleichen und Analysieren verschiedener Protokolle auf der Grundlage derselben Zeiten zu ermöglichen.
> Ereignet sich ein Vorfall, erfordert die Erstellung digitaler Bilder, das Kopieren einer grossen Anzahl von Protokollen usw. schnell eine grosse Menge an Speicherplatz (zum Beispiel externer Speicher), der bereits vorhanden sein sollte.
> Häufig werden Daten für einen bestimmten Zeitraum archiviert. Es ist ratsam, dass die Verantwortlichen für die Erstversorgung wissen, welche Archive existieren, wie sie darauf zugreifen können und in welcher Struktur Daten archiviert werden.

Organisatorische Massnahmen

> Der Umgang mit Vorfällen muss im Voraus mit klaren Verfahren, Verantwortlichkeiten und (mit der Unternehmenskommunikation erarbeiteten) Kommunikationsstrategien vorbereitet werden.
> Die interne und externe Kommunikation muss (unterstützt durch die Unternehmenskommunikation) geregelt werden. Informieren Sie Ihr technisches Team so offen wie möglich, um auf Vorfälle zeitnah und effektiv zu reagieren. Zudem sollen unerwünschte Kollateralschäden vermieden werden.
> Es ist zu empfehlen, einen aktuellen und vollständigen Bestand aller Systeme, Software und Netzwerke zu führen. Ein solches Inventar muss für alle Beteiligten direkt zugänglich sein.
> Stellen Sie eine direkte Verbindung zwischen Vorfallreaktion, Schwachstellenmanagement und Risikomanagern her, um sicherzustellen, dass alle Risiken bekannt sind und behandelt werden.
> Es ist wesentlich, die wichtigsten internen Prozesse zu kennen und einen Plan für die Weiterführung des operativen Geschäfts im Krisenfall zu haben.

Server- und Clientseite

Systemebene:

> Es ist empfehlenswert, dedizierte Systeme für die Verwaltung von Infrastrukturelementen zu verwenden. Des Weiteren soll für Administratoren/-innen eine Zwei-Faktor-Authentifizierung verwendet werden.
> Definieren Sie Erkennungsregeln für die Verwendung der Helfer-Tools der Angreifer/-innen wie psexec oder rexec.
> Eine genaue Überwachung der Ausführung von Binärdateien (Binaries) über die WMI-Schnittstelle ist ratsam.
> Mithilfe von Tools zur Integritätsprüfung können Sie unbefugte Änderungen an Systemdateien erkennen. Weiter sind sie hilfreich, um die Auswirkungen nach einem Vorfall einzuschätzen.
> Bereiten Sie die Möglichkeiten zur Überwachung und Analyse Ihres Systemspeichers vor. Dies erhöht Ihre Chance, komplexe Bedrohungen schnell zu erkennen und darauf zu reagieren.

Virtualisierung:

> Eignen Sie sich ein gewisses forensisches Wissen an. Dieses hilft Ihnen, festzustellen, ob ein VM-Ausbruch stattgefunden haben könnte.
> Die Vorbereitung von Netzwerk-Sniffing-Funktionen kann Ihnen dabei helfen, den Datenverkehr zwischen VMs zu überwachen.

Active Directory:
> Haben Sie ein klares Verständnis für die Vertrauensbeziehung zwischen verschiedenen AdForests.
> Führen Sie eine genaue Überwachung der AD-Protokolle auf ungewöhnliche und grosse Abfragen durch, die Sie nicht erwarten würden.
> Halten Sie Massnahmenpläne für den Ernstfall bereit, die ein komplett kompromittiertes Active Directory beinhalten.

Netzwerk:
> Verwenden Sie eine zentrale und gut bewachte Schnittstelle, die jedes Paket in Richtung Internet passieren muss. Dasselbe kann für den eingehenden Datenverkehr getan werden, der auf verschiedene Netzwerkzonen verteilt ist. Sie können die Einrichtung zentraler Zugriffszonen mit Load Balancers, Web Application Firewalls und Authentifizierungs-Gateways in Betracht ziehen, mit denen Sie den eingehenden Datenverkehr zentral überwachen können.
> Schauen Sie sich die Routingpfade vom internen Netzwerk zu exponierten Netzwerkbereichen, wie beispielsweise einer DMZ, genau an. Passiert dieser Verkehr obgenannte zentrale und gut bewachte Schnittstelle auch? Wenn nicht, platzieren Sie Sensoren, die auch diesen Verkehr überwachen.
> Jeder Internetzugang sollte einen Proxy passieren, der alle Header-Informationen, einschliesslich Cookies, protokolliert.
> Sammeln Sie Netflowdaten, nicht nur zwischen den Netzwerkzonen, sondern auch innerhalb der Zone.
> Verwenden Sie neben kommerziellen Lösungen auch ein klassisches signaturbasiertes IDS wie Snort oder Suricata. Es gibt Ihnen die Möglichkeit, im Falle eines Eindringens, schnell handgemachte Erkennungsregeln einzusetzen.
> Verwenden Sie Passive DNS, damit alle Domainabfragen über das Internet laufen und diese schnell und effizient auffindbar sind.

Logdateien:
> Speichern Sie die Protokolldateien so lange wie möglich. Mindestens zwei Jahre werden empfohlen, insbesondere für wichtige Systeme wie Domain Controller und Gateways.
> Protokolldateien müssen zentral gesammelt werden. Es ist empfehlenswert, ein Protokollverwaltungskonzept zu haben, das alle Netzwerkzonen abdeckt und die Indizierung, Suche und Archivierung aller Protokolldateien ermöglicht.
> Im Weiteren ist die Implementierung einer kontinuierlichen Protokollanalyse angezeigt, die einen automatisierten Abgleich dieser Protokolldateien mit bekannten IOCs ermöglicht.
> Die Protokollverwaltung ist ein laufender Prozess. Sie müssen über genügend Ressourcen verfügen, um Ihrem System ständig neue Quellen hinzuzufügen, da sich auch Ihre IT-Landschaft stets verändert.
> Passen Sie die Logeinstellungen an Ihre Bedürfnisse an. Beispielsweise ist die Protokollierung des Benutzeragenten möglicherweise nicht die Standardeinstellung, sie wird aber dringend empfohlen.
> Erfahrene Mitarbeitende sollten nicht nur die vorverarbeiteten Protokolldateien analysieren, sondern auch die Rohprotokolle auf Unregelmässigkeiten überprüfen. Dazu sollten genügend zeitliche und personelle Ressourcen eingeplant werden.

In Zusammenarbeit mit MELANI und Swiss Cyber Experts