Krisenabwehr braucht Teamwork

Arne Wöhler, Head of Business Consulting and Development Cyber Security bei Arvato Systems, **erläutert im Interview,** worauf es bei der richtigen Incident-Response-Strategie ankommt.

ITD: *Herr Wöhler, wenn es um IT-Sicherheit geht, wird in der Regel über präventive Maßnahmen gesprochen. Was aber bei einem konkreten Vorfall geschehen muss, ist vielen gar nicht klar. Woher kommt dieses Defizit?*

Arne Wöhler: Was bei einem Sicherheitsvorfall zu tun ist, hängt vom individuellen Fall ab. Im Zweifel müssen Unternehmen ihre über viele Jahre gewachsenen IT-Infrastrukturen innerhalb weniger Wochen praktisch komplett neu organisieren. Das ist mit großem Aufwand und hohen Kosten verbunden. Wenn sie nicht durch einen akuten Sicherheitsvorfall dazu gezwungen sind, gehen die allermeisten Firmen solch kostspieligen Projekten aus dem Weg. Denn auf den ersten Blick hat es den Anschein, als würden sie nur viel Geld ausgeben und Risiken eingehen, ohne einen Nutzen zu haben. Darum beschäftigen sich Verantwortliche oft erst dann mit der Thematik, wenn das Kind schon in den Brunnen gefallen ist – also wenn das Unternehmen tatsächlich angegriffen wird.

Die Abwehr *von Cyberangriffen ist laut Arne Wöhler von Arvato Systems u.a. eine Frage der richtigen Zusammenarbeit.*

ITD: *Unternehmen müssen für den Fall der Fälle also einen Plan in der Schublade haben. Bis zu welchem Grad ist dieser allgemeingültig/standardisiert und inwiefern muss er individuell auf das entsprechende Unternehmen abgestimmt werden?*

Wöhler: Für eine erfolgreiche Incident Response gibt es – wie bei jedem Krisenabwehrplan – mehrere Erfolgsfaktoren: Kommunikation, Organisation und Prozesse sowie Ressourcen. Daraus lassen sich einzelne Maßnahmenpakete präventiv ableiten und dokumentieren. Sie beschreiben das Ziel, die Vorgehensweise, die notwendigen Rollen samt involvierten Unternehmensbereichen und die nötigen Skills. Beispiele sind hier Domain Administration und Datacenter Management. Auch ein Incident-Response-Kommunikationsplan darf nicht fehlen.

Grundsätzlich lässt sich Incident Response in zwei Handlungsstränge aufteilen. Da wäre zunächst die forensische Untersuchung des vermeintlichen Vorfalls. Hier ist zu ermitteln, wie der Angreifer in die Infrastruktur eindringen konnte, welche Ziele er verfolgt, wie tief er eingedrungen ist und welche technischen Methoden er angewendet hat. Um diese Fragen zu beantworten, ziehen Analysten Logging-Daten und Informationen der möglicherweise vorhandenen Endpoint Detection sowie des Netzwerk-Monitorings heran und analysieren auffällige Systeme bis in die Tiefe. Üblicherweise konzentriert sich die Untersuchung auf die Bereiche Active Directory, DMZ – das steht für „Demilitarisierte Zone", also eine Pufferzone als eigenständiges Netzwerk zwischen internem und externem Netzwerk – und die sogenannten Kronjuwelen, also besonders schützenswerte Bereiche.

Auf Basis der Erkenntnisse geht es dann darum, Maßnahmen zur Abwehr des Angriffs und zur Entfernung des Angreifers aus dem Netzwerk zu planen. Bei laufenden Angriffen ist zu entscheiden, ob und welche Ad-hoc-Maßnahmen eingeleitet (Containment) und welche der vorbereiteten Maßnahmenpakete angewendet werden müssen. Gleiches gilt für die Vorbereitung einer Remediation und deren Durchführung. Da sich Unternehmen im Hinblick auf Komplexität, Aufbau der Infrastruktur (Domains, Netzwerk, DMZ etc.), Monitoring-Fähigkeiten auf Endpoints und Netzwerkverkehr sowie verfügbare Analyse-Skills unterscheiden, sind diese Maßnahmenpakete individuell anzupassen. Gleiches gilt für die notwendigen Abwehrmaßnahmen, die natürlich den Methoden und Techniken des Angreifers entsprechen müssen.

> „Was bei einem Sicherheitsvorfall zu tun ist, hängt vom individuellen Fall ab."

ITD: *Nach welchen Kriterien können IT-Verantwortliche einen zum Unternehmen passenden Plan erarbeiten?*

Wöhler: Es ist wichtig, die eigene Organisation, die vorhandenen Skills und die eigene Infrastruktur zu kennen. Anhand der Systemkritikalität lassen sich Kronjuwelen und neuralgische Punkte ermitteln. Was es dabei unbedingt braucht, ist Teamwork. Man kann Incident Response durchaus als eine Art Mannschaftssport betrachten, bei dem einzelne Positionen mit Spielern besetzt sind, die ihre Stärken nach vorher abgestimmten Playbooks einbringen. Für eine optimale Besetzung der Positionen braucht es einen ausgewogenen Mix aus Erfahrung und Skills. Zudem ist es für eine erfolgreiche Incident Response wirklich wichtig, mögliche Ernstfälle regelmäßig zu trainieren.

ITD: *Bei welchen konkreten Vorfällen muss ein Incident-Response-Plan schließlich greifen?*

Wöhler: Die Einschätzung, ob es sich um einen Sicherheitsfall handelt, nehmen typischerweise die Analysten des SOCs (Security Operations Center) vor. Sie bewerten das Gefahrenpotenzial und entscheiden gemeinsam mit dem Incident-Response-Team, ob ein potenzieller Verteidigungsfall vorliegt. Sollte es sich um einen massiven Sicherheitsvorfall handeln, übernimmt das Incident-Response-Team.

> „Unternehmen müssen gegen hoch entwickelte Angriffe gewappnet sein."

ITD: *Welche Rolle spielt die Nachbereitung eines Vorfalls, sobald die Gefahr gebannt ist?*

Wöhler: Einen Vorfall nachzubereiten, ist sehr wichtig. Aus einem Vorkommnis lassen sich strategische Maßnahmen ableiten, um zukünftig eine bessere Reaktionsfähigkeit und Resilienz zu entwickeln. Im Fußball würde man sagen: Nach dem Spiel ist vor dem Spiel. Hier geht es um Fragen wie: Passten Spielaufbau und Organisation? Haben alle Beteiligten mit den richtigen Skills auf den richtigen Positionen gespielt? War die Kommunikation effizient? War die Visibilität über das Spielgeschehen ausreichend? Wie sind gegebenenfalls Risikomanagement- oder Entscheidungsprozesse zu optimieren? Denn es gilt: Assume Breach! Nach dem Angriff ist vor dem Angriff. <

PHILIP FASSING, HANNAH WINTER-ULRICH

Blühendes Geschäft mit falschem Alarm

Angst ist ein Brandbeschleuniger für Kriminelle. Kein Wunder also, dass Scareware boomt. Ein neuer Bericht enthüllt, dass es die Angreifer mit ihren „Panikanzeigen" auch auf deutsche Webseiten und Mobilgeräte abgesehen haben.

> Online-Werbenetzwerke gibt es nicht ohne ihren Parasiten: bösartige Web-Banner. Besonders „Pop-under"-Werbung, die die Pop-up-Blockierungsfunktionen der Browser umgeht, ist ein Problem, denn einige dieser „Pop-unders" vermitteln ihren Nutzern sehr glaubhaft, dass etwas mit ihren Geräten nicht stimmt. Diese „Fake-Alerts" nutzen häufig Werbenetzwerke für die Verbreitung von potenziell unerwünschten Anwendungen. Und da sie keinen offensichtlich bösartigen Code enthalten, lösen die meisten keine Anti-Malware-Erkennung aus. Sie sind eine Art Scareware-Version böswilliger Werbung. Sophoslabs berichtet, dass nun vermehrt japanisch-, deutsch- und französischsprachige Benutzer ins Visier geraten. Pop-up-Blocker im Browser bieten einen gewissen Schutz, reputationsbasierte Blockierungen und Malware-Schutz können ebenfalls viele dieser Websites blockieren. Das Problem auf der mobilen Seite bleibt jedoch eine mangelnde Aufmerksamkeit der Nutzer. Während Apple und Google es Betrügern erschwert haben, Browser-Funktionen für ihre Zwecke zu nutzen, ist der Pop-up-Schutz nach wie vor schwach und der Missbrauch von App-Stores weiterhin ein Problem. Da der Schutz auf Desktops zunimmt, werden sich mehr Betrüger auf mobile Geräte konzentrieren. <

Im Internet: www.sophos.com

„Fake-Alerts" *nutzen häufig Werbenetzwerke für die Verbreitung von potenziell unerwünschten Anwendungen.*