Whitepaper

Notfallreaktion bei Sicherheitsvorfällen: 10 häufige Fehler von Sicherheits-verantwortlichen

intel Security

Ein Whitepaper von:
Michael G. Spohn
Leitender Berater
McAfee® Foundstone®
Professional Services
Reaktion auf Sicherheitsvorfälle
und forensische Verfahren

Inhalt

Einführung

Als leitender Sicherheitsexperte des Teams für Reaktionen auf Zwischenfälle und Forensik bei McAfee® Foundstone®, einem Geschäftsbereich des Intel® Security-Produkt- und Service-Angebots, hatte ich schon mit unzähligen Sicherheitsvorfällen zu tun. In den letzten Jahren war ich bei mehr als 100 Unternehmen vor Ort und unterstützte sie bei schwerwiegenden Sicherheitskompromittierungen. Die Gründe für diese Aufträge reichten von typischen Malware-Infektionen und Zwischenfällen durch Mitarbeiterfehlverhalten bis hin zu prominenten Kompromittierungen durch Gruppen wie Anonymous und LulzSec. Die meisten Zwischenfälle dieser Art umfassen eine teilweise oder vollständige Unterbrechung der Geschäftsabläufe sowie den Diebstahl von geistigem Eigentum, Geschäftsgeheimnissen, Finanzinformationen und/oder vertraulichen persönlichen Informationen.

Bei jedem dieser Aufträge lernte ich etwas, das ich noch nicht kannte. Genau auf diesem Grund finde ich die Untersuchung von Sicherheitskompromittierungen so faszinierend. Im Laufe der Zeit fielen mir Verhaltensmuster bei den Vorfallreaktionsteams auf, mit denen ich zusammenarbeitete. In fast allen Fällen schafften es diese Sicherheitsverantwortlichen nicht, die Bedrohungen effizient und wiederholbar zu beheben. Nun, wäre das anders gewesen, würde es wohl keinen Bedarf nach Unternehmen wie unserem geben.

In diesem kurzen Whitepaper möchte ich die 10 schwerwiegendsten Fehler bei der Reaktion auf Zwischenfälle vorstellen, auf die ich immer wieder stoße. Mein Ziel ist, dass Sie Ihre eigenen Sicherheitsverfahren überprüfen und selbst sehen, ob Sie diese Fehler ebenfalls machen.

Szenario des Auftrags

Bei einem typischen Auftrag ruft uns der Kunde an und fordert sofortige Hilfe bei der Eindämmung einer Sicherheitskompromittierung an. Fast immer haben wir innerhalb der folgenden 24 Stunden einen Sicherheitsexperten vor Ort.

Ich habe immer wieder festgestellt, dass sich bei einer erfolgreichen Reaktion auf Zwischenfälle folgende Dinge immer wieder zeigen:

- Die Größe des Unternehmens ist nicht relevant. In größeren Unternehmen kann es länger dauern, um einen Zwischenfall einzudämmen, doch der Ablauf ist letztendlich immer der gleiche.
- Die Branche spielt keine Rolle. Die Vorgehensweise beim Umgang mit einer Sicherheits-kompromittierung hat nichts mit der Tätigkeit des Kunden zu tun. Natürlich unterliegen bestimmte Branchen speziellen datenschutzrechtlichen und gesetzlichen Vorschriften, doch wir halten uns bei unserer Arbeit ohnehin an die strengsten Vorgaben. Das sollten Sie ebenfalls tun.
- Die Möglichkeiten von Kunden im Umgang mit Krisen können sehr unterschiedlich sein. Beispielsweise haben Behörden meist robustere Verfahren zur Krisenbewältigung als mittelgroße Rechtsanwaltskanzleien. Dennoch ist der Unterschied nicht groß genug, um ernsthafte Auswirkungen zu haben.
- Die technischen Qualifikationen von Kunden können sehr unterschiedlich sein, und das macht tatsächlich einen Unterschied. Kunden mit umfangreicher technischer Expertise (insbesondere bei der Netzwerkverwaltung) haben meist größeren Erfolg bei der Eindämmung von Sicherheitsvorfällen.
- Alle Unternehmen zeigen unter Druck ein bestimmtes Verhaltensmuster.

Diese Liste soll Ihnen zeigen, dass ein ausgereifter und strukturierter Ansatz bei der Reaktion auf Zwischenfälle auch Ihrem Unternehmen einen großen Vorteil bringt.

Die 10 schwersten Fehler

1. Niemand ist verantwortlich
Ich kann gar nicht oft genug betonen, wie wichtig es ist, dass ein Mitarbeiter für die Koordination der Reaktionen auf Zwischenfälle verantwortlich ist. In den letzten zehn Jahren wechselten die Unternehmen zu eher dezentralisierten Verwaltungsstrukturen. Die Verantwortungsbereiche sind eher unscharf definiert, und geografische Grenzen sind verschwunden.

Der für die Reaktion auf Zwischenfälle eingesetzte Mitarbeiter hat die übergeordnete Verantwortung für eine Eindämmung von Sicherheitsvorfällen. Ich werde manchmal gebeten, diese Rolle zu übernehmen. Allerdings bin ich der Meinung, dass ein interner Mitarbeiter diese Position übernehmen sollte. Ein leitender Manager oder Abteilungsleiter ist dafür meist die beste Wahl. Führungskräfte der obersten Ebene übernehmen nur sehr selten diese Rolle, obwohl die Verantwortlichen noch nicht einmal über höhere technische Kenntnisse verfügen müssen. Viel wichtiger sind Kommunikation, Organisation und die Fähigkeit, Aufgaben zu delegieren.

2. Fehlende Leitstelle
Viel zu häufig versuchen Unternehmen, ernsthafte Zwischenfälle über Telefonkonferenzen, Mobiltelefonen und E-Mails zu lösen. Glauben Sie mir: Das funktioniert nicht. Ein zentraler Konferenzraum oder ein Büro sollten als Leitstelle festgelegt werden.

Der gewählte Ort sollte groß genug sein, um ein Dutzend Personen aufzunehmen, mit großen Whiteboards oder Wandtafeln für Notizzettel sowie einem Telefon mit Konferenzfunktion bzw. Lautsprecher ausgestattet sein und eine Möglichkeit zur Zugangsbeschränkung bieten. Dabei sollte der Zugang auf die Personen beschränkt werden, die mit dem Zwischenfall direkt zu tun haben. Die Leitstelle fungiert als zentrale Schnittstelle für die gesamte Kommunikation, die Planung der Eindämmungsmaßnahmen, die Aufgabendelegierung sowie für Status-Updates.

3. Fehlende Möglichkeit zum Aufspüren und Identifizieren des Gegners
Auf die Frage dazu, was sie bei unseren Notfall-Services besonders schätzen, nennen unsere Kunden meist die Fähigkeit zum Krisen-Management sowie den Umgang mit Bedrohungen. Das Bedrohungs-Management umfasst die Aufdeckung der Quelle sowie der Vorgehensweise der Bedrohung.
Wir nennen das „Kenne deinen Gegner“. Dieser Ansatz ist nicht sonderlich kompliziert, doch viele Kunden haben damit Schwierigkeiten.

Was wir jeweils unter dem Gegner verstehen, ist abhängig von der Art des Zwischenfalls. Wichtig ist, die Bedrohung aufzudecken und klar zu erkennen, wie sie wirkt. Beispielsweise besteht unsere Vorgehensweise beim Auffinden und Kennenlernen des Gegners aus den folgenden Schritten:

- Identifizierung des Angriffsvektors
- Durchführung einer forensischen Live-Analyse
- Isolierung des Hosts und Extraktion von Malware-Exemplaren
- Erstellung eines Profils der Malware und Erkennung der Kommunikationsmethoden
- Einreichung von Malware-Exemplaren an den Virenschutz-Anbieter
- Nutzung von Virenschutz-Tools für Unternehmen

Glauben Sie mir: Sie verfügen erst dann über eine effektive Strategie zur Eindämmung von Zwischenfällen, wenn Sie Ihren Gegner kennen.

4. Fehlen eines ausgearbeiteten Eindämmungsplans
Wenn ich bei einem Sicherheitsvorfall vor Ort eintreffe, bin ich immer wieder auf's Neue von den chaotischen Zuständen überrascht. Nur wenige Unternehmen haben einen Plan zum Umgang mit Krisen ausgearbeitet und dokumentiert, sodass wir als erstes diese Aufgabe übernehmen. Meist erstelle ich innerhalb der ersten vier Stunden der Abwehr einer Sicherheitskompromittierung ein ein- bis zweiseitiges Dokument mit einer kurzen Auflistung der strategischen Maßnahmen zur Eindämmung von Zwischenfällen. Dieser Eindämmungsplan ist eine wichtige Komponente der McAfee Foundstone-Methodik zur Reaktion auf Sicherheitsvorfälle. Deshalb verzichten wie nie darauf, einen zu erstellen.

Im Wesentlichen besteht diese Methodik aus folgenden Schritten:

- Feststellung des Angriffsvektors und Umfangs des Sicherheitsvorfalls
- Kenne den Gegner – Identifizierung seiner Tools und Taktiken
- Gemeinsame Ausarbeitung und Dokumentation einer Eindämmungsstrategie
- Erstellung einer Aufgabenliste basierend auf dem Eindämmungsplan
- Delegierung und Überwachung von Aufgaben, bis die Eindämmung erfolgt ist

5. Fehlende Dokumentierung
Ich geb's zu: Ich bin ein Vertreter der alten Schule, der noch ein Notizbuch mit sich herumträgt. Die Zeiten haben sich aber geändert. Die jungen Menschen von heute kennen keine Welt ohne Elektronik mehr. Die Nutzung von Textnachrichten und E-Mails hat die Bedeutung von Dokumentation verändert. Das führt auch dazu, dass viele Sicherheitsverantwortliche vergessen haben, wie wichtig gute Dokumentation ist.

Ein Helpdesk-Ticket-System genügt nicht, um einen Vorfall zu dokumentieren. Stattdessen empfehlen wir allen Sicherheitsverantwortlichen, stets ein Notizbuch mit sich zu führen und alle Aktionen aufzuschreiben. Alle Ereignisse und delegierten Aufgaben sollten dokumentiert und an einem zentralen sowie sicheren Ort aufbewahrt werden.

6. Fehlende Ausarbeitung einer Chronologie des Sicherheitsvorfalls
Meiner Ansicht nach ist die Erstellung der Chronologie eines Sicherheitsvorfalls eine der wichtigsten Aufgaben bei dessen Abwehr. Das bedeutet in erster Linie, dass Sie die Ereignisse dokumentieren und nach Datum/Uhrzeit von alt bis neu sortieren müssen. Ihre Liste muss keinen Schönheitspreis gewinnen, sondern soll einfach nur vollständig und aktuell sein.

Eine detaillierte Chronologie des Sicherheitsvorfalls stellt einen Wegweiser für Ihre Eindämmungsstrategie dar. Sie bringt Klarheit in komplexe Untersuchungen und hilft Ihnen, sich auf das große Ganze zu konzentrieren. Außerdem ist sie eine wunderbare Möglichkeit, Führungskräften im Nachhinein die Vorgänge zu erklären.

7. Verwechslung von Eindämmung mit Behebung
Ein sehr häufiger Fehler von Unternehmen ist die Verwechslung von Eindämmung mit Behebung. Sie agieren nur dann effektiv, wenn Sie die Bedrohung zuerst eindämmen und im zweiten Schritt beheben. Warum? Während der Eindämmung konzentrieren Sie sich darauf, eine Bedrohung aufzuhalten, während sich die Behebung um die Schließung von Schwachstellen dreht. Stellen Sie sich einen Sicherheitsvorfall als Gebäudebrand vor. In diesem Fall konzentrieren Sie sich mit allen Mitteln darauf, das Feuer zu ersticken. Das Dach hingegen wird erst im Anschluss repariert.

Die Notfallreaktion bei Sicherheitsvorfällen ist ein Eindämmungsprozess. Es ist absolut notwendig, dass jedes Mitglied Ihres Vorfallreaktionsteams versteht, dass die Eindämmung an erster Stelle steht. Alle anderen Aufgaben, die damit nicht in unmittelbarem Zusammenhang stehen, sollten auf einen späteren Zeitpunkt verschoben werden.

8. Fehlende Überwachung und Absicherung der Netzwerkperipherie
Ich bin immer wieder überrascht, dass nur wenige Unternehmen Technologien zur Netzwerküberwachung nutzen. Wenn Sie nicht wissen, welcher Datenverkehr in Ihren Netzwerken übertragen wird, können Sie auch keine Netzwerk-basierten Bedrohungen abwehren. Ich kann die Bedeutung der Absicherung Ihrer Netzwerkperipherie und der Überwachung des ausgehenden Netzwerkverkehrs nicht genug betonen.

Warum ausgerechnet ausgehender Datenverkehr? Weil Ihr Gegner Ihre vertraulichen Daten von Ihrem Netzwerk in seines übertragen muss. Bei einer Sicherheitskompromittierung konzentrieren wir uns stets zuerst auf die Absicherung der Netzwerkperipherie und arbeiten uns anschließend nach innen vor. Die Absicherung der Peripherie nimmt Ihrem Gegner die Möglichkeit zu Kommunikation. Sobald das geschafft ist, können wir uns von der Peripherie nach innen arbeiten, um die Tools des Gegners zu finden und zu beseitigen.

9. Unzureichende Protokollierung
Um es mit aller Deutlichkeit zu sagen: Die überwiegende Mehrheit der Unternehmen, von denen wir zu Hilfe gerufen werden, besitzt keine ausreichenden Protokollierungsmechanismen. Aus Gründen, die ich nicht nachvollziehen kann, ist der Widerstand gegen eine effektive Protokollierung auch weiterhin ungebrochen. Wir müssen diese Einstellung ändern, denn Protokolle sind in den meisten Fällen die effektivste Quelle für Beweise. Meiner Erfahrung nach sind die wertvollsten Protokolle die der Netzwerkperipherie.

Daher benötigen effektive Vorfallreaktionsteams schnellen Zugriff auf Protokolldateien einschließlich den folgenden:

- Systemprotokolle oder andere zentralisierte Protokolle
- Firewall-Protokolle, Eindringungserkennungs- und -schutzsysteme (IDS/IPS)
- Web-Proxy-Protokolle
- Microsoft Windows-Ereignisprotokolle
- VPN-Protokolle
- DHCP-Protokolle
- DNS-Protokolle
- Microsoft Active Directory (AD)-Protokolle
- Unternehmens-AD-Protokolle

10. Verwaiste Virenschutz-Systeme im Unternehmen
Dieser Fehler könnte Sie überraschen. In der Sicherheits-Community herrscht die Meinung vor, dass moderne Virenschutz-Systeme im Unternehmen keinen effektiven Schutz mehr vor aktuellen hochentwickelten und polymorphen Bedrohungen bieten. Doch auch wenn wir die Schlacht an dieser Front verlieren, sind Ihre Unternehmens-Virenschutz-Systeme noch immer eine wichtige Komponente Ihres Verteidigungsarsenals. Tatsächlich kamen bei der Abwehr der meisten Malware-Infektionen oder APT-Zwischenfälle, mit denen ich in den letzten vier Jahren zu tun hatte, Virenschutz-Systeme für Unternehmen zum Einsatz.

Wenn Unternehmen ihre Virenschutz-Tools nicht nutzen, kommen sie in Teufels Küche. Zu den häufigsten Fehlern in diesem Bereich gehören:

- Fehlende Überwachung und/oder Durchsetzung der Virenschutz-Compliance
- Veraltete Agenten
- Veraltete Signaturen (DAT-Dateien)
- Fehlende tägliche Kontrolle der Virenschutz-Systeme
- Fehlende Erstellung automatisierter Ereigniswarnungen
- Fehlende Überwachung von Warnungen des Virenschutz-Anbieters

Zusammenfassung

Dies ist sie, die Liste der 10 häufigsten Fehler, die ich immer wieder bei Sicherheitsverantwortlichen beobachte. Wie Sie sehen, lässt sich jeder dieser Fehler ohne große Schwierigkeiten korrigieren. Tatsächlich kann Ihr Unternehmen die Effektivität Ihrer aktuellen Maßnahmen zur Reaktion auf Sicherheitsvorfälle überprüfen. Bei McAfee Foundstone haben wir uns ganz der Sicherheit verschrieben. Wir unterstützen Unternehmen dabei, ihre Sicherheitslage zu verbessern, was am einfachsten durch präventive Maßnahmen zu erreichen ist. Unser Ratschlag: Scheuen Sie nicht den Zeitaufwand, und überprüfen Sie, ob Ihr Notfallreaktionsplan aktuell und effektiv ist.

Informationen zum Autor

Michael Spohn ist leitender Sicherheitsberater bei McAfee Foundstone, wo er bei Kunden Maßnahmen zur Notfallreaktion sowie digitale Forensik durchführt. Seine Aufgaben umfassen die Erstellung von Verwaltungsprogrammen zur Notfallreaktion, Analyse und Tests bestehender Notfallreaktionspläne sowie die Durchführung forensischer Untersuchungen und Notfallreaktions- sowie Forensikschulungen. Er gehört auch zum Notfallreaktionsteam von McAfee Foundstone, das Kunden Notdienste bei Sicherheitskompromittierungen mit erhöhtem Schweregrad anbietet.

Über McAfee Foundstone Professional Services

McAfee Foundstone Professional Services, eine Abteilung von McAfee (einem Geschäftsbereich von Intel Security), unterstützt Unternehmen mit Expertendiensten sowie Schulungsmaßnahmen zum kontinuierlichen und spürbaren Schutz ihrer wichtigsten Ressourcen auch vor den gefährlichsten Bedrohungen. Dank eines strategischen Ansatzes an die Sicherheit erkennt und implementiert McAfee Foundstone das richtige Gleichgewicht aus Technologien, Mitarbeitern sowie Prozessen, um digitale Risiken zu kontrollieren und Sicherheitsinvestitionen effektiver zu nutzen. Das professionelle Serviceteam besteht aus anerkannten Sicherheitsexperten und Autoren, die über umfassende Sicherheitserfahrung in multinationalen Unternehmen, dem öffentlichen Sektor sowie dem US-Militär verfügen. **http://www.mcafee.com/de/services/mcafee-foundstone-practice.aspx**

Über Intel Security

McAfee ist jetzt ein Geschäftsbereich von Intel Security. Durch die Security Connected-Strategie, einen innovativen Ansatz für Hardware-unterstützte Sicherheitslösungen sowie das Global Threat Intelligence-Netzwerk ist Intel Security voll und ganz darauf konzentriert, für die Sicherheit seiner Kunden zu sorgen. Dazu liefert Intel Security präventive, bewährte Lösungen und Dienste, mit denen Systeme, Netzwerke und Mobilgeräte von Privatanwendern und Unternehmen weltweit geschützt werden können. Intel Security verknüpft die Erfahrung und Fachkompetenz von McAfee mit der Innovation und bewährten Leistung von Intel, damit Sicherheit als essentieller Bestandteil jeder Architektur und Computerplattform eingebettet wird. Intel Security hat sich zum Ziel gesetzt, allen – Privatpersonen ebenso wie Unternehmen – die Möglichkeit zu geben, die digitale Welt absolut sicher nutzen zu können. **www.intelsecurity.com**

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com