Anatomie eines Angriffs

Wie Hacker eindringen – und wie Sie zurückschlagen können

Ein Cyberangriff kann Ihr Unternehmen Millionen kosten. Haben Sie den richtigen Plan aufgestellt, um einem Angriff stand zu halten, ihn zu lindern und sich davon zu erholen?

Microsoft

INHALT

03 **Einführung:**
Die vier Phasen eines Angriffs

04 **Phase eins:**
Den Fuß in die Tür bringen

05 **Branchenprofil:**
Gesundheitswesen

07 **Phase zwei:**
Mehr Kontrolle erlangen

08 **Branchenprofil:**
Unterhaltungsmedien

10 **Branchenprofil:**
Nahrungsmittelherstellung

12 **Phase drei:**
Expansion auf das Netzwerk

13 **Branchenprofil:**
Regierungsbehörden

15 **Phase vier:**
Festsetzung für eine lange Persistenz

16 **Branchenprofil:**
Hightech-Herstellung

18 **Branchenprofil:**
Internet-Einzelhandelsunternehmen

20 **Schlussfolgerung:**
Schützen, Auffinden, Reagieren

Einführung

Die vier Phasen eines Angriffs

Die vier Phasen eines Angriffs

Sicherheitsbedrohungen sind unnachgiebig. Cyberangriffe können Millionen Dollar Schaden für Ihr Unternehmen und dessen Ruf verursachen, bevor Sie sie auffinden. Sind Sie sich der potenziellen Bedrohungen für Ihr Unternehmen bewusst? Und haben Sie einen Plan aufgestellt, um den vier Phasen eines Angriffs stand zu halten, sie zu lindern und sich davon zu erholen?

Lesen Sie weiter, um mehr über die einzelnen Phasen zu erfahren und um reale Beispiele der Schadensarten einzusehen, die die Angreifer während der einzelnen Phasen anrichten. Sie lernen zudem, wie Sie eine Verteidigungsstrategie gegen einen fingierten Angriff formulieren, um sich selbst und Ihr Unternehmen zu schützen.

Phase eins:
Einen Fuß in die Tür bringen

Phase zwei:
Mehr Kontrolle erlangen
(lokale Ausweitung der Berechtigungen)

Phase drei:
Expansion auf das Netzwerk
(Ausweitung der Berechtigungen
in Active Directory)

Phase vier:
Festsetzung für eine lange Persistenz

Phase eins: Den Fuß in die Tür bringen

Die kleinste Sicherheitslücke kann es einem Angreifer ermöglichen, den Fuß in Ihr Unternehmen zu bringen. Ob über einen manipulierten Arbeitsplatz, einen nicht gepatchten Server mit Internetzugang oder ein schlecht konfiguriertes Gerät, das von Dritten verwaltet wird – ein Angreifer kann und wird alle verfügbaren Mittel nutzen, um die Abwehrmaßnahmen eines Unternehmens zu durchbrechen und Zugriff auf das Netzwerk zu erhalten. Sobald der Hacker sich im System befindet, kann er es erkunden, um wertvollen Informationen oder Ressourcen Ihres Unternehmens zu finden und anzusteuern.

Gängige Begriffe:

Phishing: Eine Möglichkeit, Benutzer dazu zu verleiten, persönliche, finanzielle oder unternehmensspezifische Informationen preiszugeben, die dazu verwendet werden können, nicht autorisierten Zugriff auf die interne Infrastruktur zu erhalten. Angreifer verwenden möglicherweise Scheinwebsites oder -E-Mails, die aussehen, als wären sie von einem vertrauenswürdigen Kontakt (Beispiel: von Drittanbietern oder internen Mitarbeitern), um Benutzer dazu zu verleiten, auf bösartige Weblinks, Dokumente und andere Infektionsherde zu klicken.

Watering hole: Eine spezifische Website, von der die Angreifer herausgefunden haben, dass sie von ihrer Zielperson häufig besucht wird. Der Angreifer platziert böswillige Links zu Schadsoftware auf der Website in der Hoffnung, dass die Zielperson infiziert wird, wenn sie diese Website aufruft.

Malware: Diese Programme führen unerwünschte Aktionen auf Ihrem PC durch, wie etwa Informationsdiebstahl, Sperren des PCs bis zur Zahlung eines Lösegelds oder Verwenden des PCs zum Senden von Spam. Viren, Würmer und Trojaner sind Arten von Schadsoftware. (Dieses Dokument konzentriert sich auf sogenannte gezielte Malware. So soll eine spezifische Branche oder Organisation infiltrieren.)

Exploit: Ein Codeausschnitt, der Softwareschwachstellen für den Zugriff auf Informationen auf Ihrem PC oder zur Installation von Schadsoftware nutzt.

Zero-Day: Ein Software-Exploit, der vom Softwarehändler nicht offengelegt oder gepatcht wurde.

Branchenprofil: Gesundheitswesen

Das Gesundheitswesen hat in den letzten Jahrzehnten durch die Fusion von Krankenhäusern eine bedeutende Konsolidierung erfahren. Auch wenn die Konsolidierung aus der Sicht des Gesundheitswesens erfolgreich verlaufen ist, schafft der Prozess einer Fusion häufig technologische Herausforderungen für das Personal. Neu fusionierte Krankenhäuser entscheiden sich möglicherweise für die Reduzierung ihrer gesamten Technologieinvestitionen durch Zentralisieren der IT-Dienste in einer einzelnen Abteilung.

Der Prozess des Fusionierens von Netzwerken, Infrastruktur und Software kann zu einem Angriff führen, falls der Prozess nicht richtig durchgeführt wird. Angreifer beginnen in der Regel mit dem Netzwerk mit der schwächsten Sicherheit. Sobald sie drinnen sind, können sie interne Sicherheitslücken nutzen, um Zugriff zu einem sichereren Netzwerk zu erhalten. In einem echten Fall gelangte ein Angreifer in ein Netzwerk und knackte dann per E-Mail das Netzwerk eines anderen Krankenhauses. Das Krankenhaus bemerkte den Fehler, als ein Upgrade Stabilitätsprobleme auf seinen Servern verursachte. Die Techniker fanden eine seit langem installierte Schadsoftware, die die Kompromittierung des Netzwerks ermöglichte.

Viele Faktoren haben zu dem gesamten Angriff beigetragen. Das Krankenhaus hat sein Netzwerk nicht von anderen Organisationen getrennt und dadurch den Angreifern ermöglicht, durch das schlechter geschützte Netzwerk einzudringen. Im gesamten Netzwerk wurden gemeinsame Anmeldeinformationen verwendet und erleichterten Angreifern den Zugriff auf verschiedene Bereiche, sobald sie drinnen waren. Außerdem wurden intern entwickelte, veraltete Anwendungen mit zu niedrigen Berechtigungen betrieben. Es brauchte mehrere Jahre, um das Netzwerk neu zu gestalten und aufzubauen, sowie einen Paradigmenwechsel, um es wieder freizugeben.

Sobald ein Fuß in der Tür ist, wird die Aufgabe des Angreifers einfacher. Der Eintritt in ein Netzwerk über einer diese Methoden ermöglicht einem Angreifer den Zugang zu wichtigeren Anmeldeinformationen, die ihm neue, möglicherweise noch vertraulichere Bereiche des Netzwerks eröffnen.

Ein wenig Prävention...

Stärkere Sicherheitsmaßnahmen, wie etwa Schulungen des Personals und die Implementierung von richtigen Technologielösung, können Krankenhausnetzwerken helfen, ihre Integrität zu bewahren.

Wir empfehlen die folgenden präventiven Maßnahmen:

Implementieren Sie eine solide Basis an Industriesicherheitsrichtlinien: Trennen Sie Netzwerke, forcieren Sie hohe Kennwortanforderungen, befolgen Sie das Konzept der Mindestberechtigungen und fordern Sie individuelle Kennwörter für jedes Netzwerk und jeden Zugangsbereich. Dies ist insbesondere für ältere Geräte entscheidend, die anfällig für Angriffe sind, aber nicht mehr gepatcht werden können.

Aktualisieren Sie die Netzwerke: Halten Sie die Netzwerkinfrastruktur auf dem neuesten Stand, um zu gewährleisten, dass Sie über die neuesten Sicherheitsfeatures verfügen.

Verwenden Sie Lösungen mit integrierter Garantie: Der Health Insurance Portability and Accountability Act (HIPAA) von 1996 gilt für alle US-Unternehmen im Gesundheitswesen und etabliert Anforderungen für die Nutzung, Offenlegung und den Schutz persönlich identifizierbarer Informationen über den Gesundheitszustand. Die Cloud-Dienste von Microsoft sind mit dem HIPAA und dem Advanced Threat Protection in Windows 10 kompatibel und Office 365 scannt automatisch sämtliche Anhänge und Links in eingehenden E-Mails auf potenzielle Bedrohungen. Fragwürdiges Material erreicht die Endbenutzer nicht. Dadurch werden die Social Engineering-Bedrohungen für Ihr Netzwerk reduziert.

Phase zwei: Mehr Kontrolle erlangen

Sobald ein Angreifer ein Unternehmen infiltriert hat, ist der nächste Schritt die lokale Eskalation der Berechtigungen. Angreifer suchen in der Regel nach einer Möglichkeit zur Konsolidierung ihrer Kontrolle über das lokale System oder nach einem anderen System, das eine bessere Erfolgschance für das Erlangen der Administratorrechte oder besseren Zugang zu wertvollen Daten bietet. Das Ziel der Angreifer ist die Identifizierung der Benutzerkonten, die für die Verwaltung des Systems zuständig sind, um sich als die Person auszugeben, die die Systemressourcen verwaltet, aktualisiert und aufruft. Dann versucht der Angreifer mit integrierten und heruntergeladenen Tools, andere interessante Systeme und Netzwerkressourcen auszumachen und Benutzernamen und Kennwörter abzufangen. Diese Aktionen können in der Regel als normaler Benutzer nicht erfolgreich durchgeführt werden.

Gängige Begriffe:

Keylogger: Schadsoftware, die aufzeichnet, welche Tasten ein Benutzer drückt. Auch als **Keystroke Logging** bezeichnet. Die Aufzeichnung von Tastenanschlägen zum Abfangen von Benutzernamen und Kennwörtern, um sich im Netzwerk der Zielorganisation einzuloggen.

Pass the Hash (PtH): Eine Technik, bei der ein Angreifer den grundlegenden Hash (Code) des Kennworts eines Opfers verwendet, um sich als dieser Benutzer auszugeben. Der Angreifer muss keine tatsächlichen Benutzeranmeldeinformationen kennen, um sich an einem Remoteserver/-dienst zu authentifizieren.

Scannen eines Netzwerks: Angreifer verwenden diese Erkundungstechnik, um die derzeit zugänglichen Systeme zu katalogisieren, wie etwa Hostcomputer, Dienste und Ressourcen, die in einem Netzwerk aktiv sind. Die Angreifer erstellen dann eine Zielliste interessanter Systeme, die sie mit den neu gewonnenen administrativen Zugriffsrechten aufzurufen versuchen.

Branchenprofil: Unterhaltungsmedien

Nehmen Sie eine vielbeachtete Branche, fügen Sie kontroverse Inhalte hinzu und Sie erhalten ein Ziel für Hacker. Angriffe auf Medien- und Unterhaltungsorganisationen werden oft ebenso vom Verlangen getrieben, ein Statement abzugeben wie Informationen zu stehlen. Frühere Hackerangriffe haben Chaos verursacht, da vertrauliche Unternehmensinformationen veröffentlicht oder die Websites eines Unternehmens übernommen wurden.

In einem derartigen Fall hat ein Unternehmen einen Angriff erlitten, der nicht nur seinen Betrieb unterbrach, sondern auch vertrauliche Daten über Mitarbeiter, Kunden und geistiges Eigentum preisgab. Auch wenn nicht vollständig bekannt ist, wie dieser Angriff ursprünglich erfolgte, sind ähnliche Fälle von bekannten Angriffsvektoren wie Social Engineering, nicht gepatchten Sicherheitslücken und einfachen Fehlkonfigurationen entstanden.

Für ein Medienunternehmen kann der Schaden weitreichend sein. Das Ausmaß und die wahrscheinlichen Auswirkungen dieses Angriffs - finanzieller und geopolitischer Natur- waren zuvor noch nie dagewesen. Neben den erheblichen Kosten für die Suche und Abwehr des tatsächlichen Angriffs entstehen weitaus umfangreichere Schäden für den Ruf des Unternehmens: Es muss jetzt Zeit und Geld für die Wiederherstellung von Beziehungen aufbringen, die besser in die Entwicklung neuer Projekte investiert wären.

Eine siegreiche Netzwerklösung

Die Entwicklung einer stärkeren Sicherheitsstrategie kann helfen, verheerende Angriffe abzuwehren. Ein wichtiger Teil davon ist ein umfangreiches Risikomanagement. Das beinhaltet die Kenntnis über die vorhandenen Ressourcen, der potenziellen Risiken für diese Ressourcen, der Kosten für das Unternehmen, wenn die Ressourcen gestohlen werden, und der vorhandenen Steuerelemente, die diese Ressourcen schützen sollen. Es ist zudem entscheidend, das Auftreten eines Problems zu erkennen, es einzudämmen und effektiv auf die Folgen zu reagieren. Diese Ansätze müssen als Teil des Lebenszyklus der Sicherheit innerhalb eines Unternehmens gesehen werden, in der das Risiko stets bewertet wird und gelernte Lektionen in das System einfließen.

Wir empfehlen folgende Sicherheitsmaßnahmen:

Schützen, Auffinden, Reagieren: Dieser Ansatz hilft beim Aufbau eines Rahmens schützender Systeme und ist einer der Ansätze, die Microsoft und andere Unternehmen verfolgen, um Risiken zu erkennen, mit möglichen Angriffen umzugehen, diese abzuwehren und daraus zu lernen.

Implementierung des Zugriffs mit Mindestberechtigungen: Definieren Sie die Zugangskontrollen Ihres Netzwerks auf Grundlage der Rollen statt individueller Arbeitsstile und schränken Sie dann den Zugriff auf die Mindestberechtigungen ein, die erforderlich sind, um die zugewiesenen Pflichten und Aufgaben zu erfüllen. Falls eine Einzelperson für ihre Aufgabe keinen Zugriff auf ein Netzwerk oder eine Ressource benötigt, gewähren Sie diesen nicht. Dies ist eine gängige Methode, Angriffe einzudämmen.

Security Development Lifecycle: Dieser Softwareentwicklungsprozess hilft Entwicklern beim Erstellen sicherer Software- und Adresssicherheitsanforderungen und gleichzeitig beim Reduzieren der Entwicklungskosten.

Sowie das Bereitstellen folgender Tools:

Local Administrator Password Solutions (LAPS): Diese Lösung kann verwendet werden, um ein anderes, willkürliches Kennwort auf jedem Computer innerhalb einer Domäne festzulegen. Anschließend können sie von Domänencontroller verwendet werden, um zu bestimmen, welche Benutzer (z. B. Helpdeskadministratoren) autorisiert sind, um Kennwörter zu lesen.

Windows 10 Credential Guard: Dieses auf Virtualisierung basierende Sicherheitstool wurde in Windows 10 Enterprise eingeführt und isoliert Geheimnisse, sodass nur privilegierte Systemsoftware darauf zugreifen kann.

Microsoft Advanced Threat Analytics (ATA): Hilft Ihnen beim Erkennen von PtH-Angriffen und Bedrohungen mithilfe der Verhaltensanalyse. Die Konformitätsanforderungen an sichere Software- und Adresssicherheitsanforderungen bei gleichzeitiger Reduzierung der Entwicklungskosten.

Branchenprofil: Nahrungsmittelherstellung

Ein großer Getränkekonzern wusste, dass er seine Netzwerksicherheit verbessern und seine IT-Kosten senken musste, wusste aber nicht, wo er anfangen sollte. Er entschloss sich für ein Outsourcen der IT und die Konzentration auf sein Kerngeschäft: die Herstellung von Erfrischungsgetränken. Das Outsourcen der Arbeit an ein IT-Unternehmen hätte die Unternehmensdaten sicherer machen sollen. Stattdessen hat sich der Getränkehersteller daran die Finger verbrannt. Der Anbieter hat die Due-Diligence-Prozesse beim Schutz der wichtigen Konten des Kunden nicht eingehalten. Er konnte zudem die hohe Integrität bei den hochwertigen Konten des Kunden nicht aufrechterhalten, die auf hochwertige Server zugriffen.

In diesem Fall waren diese Konten normalen Angriffen ausgesetzt, wie Social Engineering durch Mitarbeiter-E-Mails beim Anbieter und Zufallsergebnissen beim Surfen im Internet, da der IT-Anbieter die Konten des Getränkekonzerns nicht von den normalen Aktivitäten des Anbieters trennte. Als der Angreifer Zugang zu den Konten des Getränkekonzerns erhielt, konnte er das Unternehmen genau wie der IT-Anbieter remote verwalten. Noch schlimmer war, dass der Getränkekonzern über den IT-Anbieter reagieren musste, da die Backbonesysteme des Kunden nicht mehr lokal waren. Dies erschwerte die Koordination der Untersuchung und die Behebung, bis diese wichtigen Konten wieder unter Kontrolle durch das Wartungsteam gebracht wurden.

Einige kritische Workloads konnten ausgelagert werden, während das Getränkeunternehmen die Hand auf seine Daten und der Backbone Systeme innerhalb der Organisation behielt. Die Kosten konnten ohne Auslagerung reduziert werden, indem einige Unternehmenssysteme in die Cloud ausgelagert wurden (Beispiel: durch Ersetzen einer lokalen E-Mail-Bereitstellung durch eine gehostete und verwaltete Lösung wie Office 365), während sich die internen Arbeitsabläufe auf die grundlegende Fertigung konzentrierten. Eine gehostete Lösung hilft bei der Reduzierung der Arbeitslast der Mitarbeiter, schafft vorhersagbare monatliche Kosten, bewahrt die Kontrolle über die Geschäfte und nutzt die Kompetenz eines Dienstanbieters.

Falls die Umgebung viele Systeme mit überschüssiger Kapazität enthält, sollte das Unternehmen einen Wechsel zu einem vertrauenswürdigen Cloud-Dienst in Betracht ziehen. Die Cloud bietet eine vollständige Plattform, Infrastruktur und Dienste, ohne alle Systeme und Rechenzentren einrichten und pflegen zu müssen. Das Unternehmen muss kein Patchen und Pflegen von Betriebssystemen und Hardware verwalten.

Es ist immer wichtig, Outsourcing- oder Cloud-Dienstanbietern Fragen über ihre Vorgehensweisen und Richtlinien im Hinblick auf Datensicherheit, Datenschutz und -kontrolle, Konformität und Transparenz zu stellen. Wenn das Getränkeunternehmen die Risiken bei den Sicherheitsvorkehrungen des Outsourcing-Unternehmens erkannt hätte, hätte es eine fundiertere Entscheidung darüber treffen können, wem es sein Vertrauen schenkt.

Erfolgsrezept

Das Auslagern von IT-Funktionen kann eine attraktive Lösung im Hinblick auf die Reduzierung des Aufwands darstellen. Sie müssen jedoch herausfinden, ob die Auslagerung der IT den besten Schutz Ihrer Unternehmensdaten und des geistigen Eigentums bietet, und dann einen Händler oder Dienstanbieter wählen, dessen Richtlinien und Praktiken Ihr Vertrauen verdienen. Wie das Getränkeunternehmen herausfand, müssen die Vorteile des Auslagerns das Risiko aufwiegen, dass Ihre Datensicherheitsanforderungen in Händen eines externen Unternehmens liegen.

Wir empfehlen, vor der Suche nach einem Anbieter die folgenden Fragen zu stellen:

- **Welche Arten von Diensten sollen wir auslagern?**
- **Welche Zugriffsebenen sollen wir auslagern?**
- **Wie können wir die Cloud zur Reduzierung der IT-Kosten verwenden (statt sie an Dritte auszulagern)?**

Nach dem Überprüfen Ihrer Situation können Sie bestimmen, dass ein externer Anbieter oder ein Cloud-Dienstanbieter die beste Option ist. Prüfen, untersuchen und hinterfragen Sie den potenziellen Anbieter gründlich. Stellen Sie ihm Fragen und finden Sie heraus, ob er für den Notfall eine Versicherung hat.

Stellen Sie Ihrem potenziellen Anbieter die folgenden Fragen:

- **Befolgen Sie die bewährten Vorgehensweisen im Hinblick auf Enhanced Security Administrative Environment (ESAE)?**
- **Gibt es Einschränkungen, ob Domänenadministrator- und Unternehmensadministrator-Konten sich anmelden können?**
- **Verwenden Sie die privilegierte Identitätsverwaltung für Active Directory Azure?**

Phase drei: Expansion auf das Netzwerk

In Phase drei erhält der Angreifer weitreichenden Zugriff auf Ihr Netzwerk, indem er sich von einem einzelnen Arbeitsplatz oder einem einzelnen Server auf möglichst viele Systeme ausbreitet. Der Angreifer kann dann eine dauerhafte Hintertür oder einen alternativen Mechanismus für den langfristigen Zugriff auf die Systeme installieren.

Die Angreifer verwenden Tools, einige davon sind möglicherweise Schadsoftware (sogenannte Implantate). Einige Methoden können legitimer erscheinen, wie etwa das Erstellen von Scheinkonten und das Erlangen von Remotezugriff, damit der Angreifer mehrere Möglichkeiten hat, nicht nur zurück ins Netzwerk zu kommen, sondern auch, um sich in der Umgebung zu verstecken und verschiedene andere Ressourcen aufzurufen. In der Regel haben Angreifer bei der Verwendung von Implantaten und Bots eine Befehls- und Steuerkonsole für alle Ressourcen, die sie kontrollieren. Sie verwenden die Befehls- und Steuerkonsole, um zu gewährleisten, dass sie im gesamten Netzwerk Fuß fassen. Falls Sie feststellen, dass einer der Zugänge, den Sie kontrollieren, systemgesteuert offline geht, wissen Sie, dass jemand auf Ihrer Fährte ist und versuchen kann, seinen Zugang wiederherzustellen und den Angriff abzuwehren.

Gängige Begriffe:

Bots: Kleine, versteckte Programme, die von einem Angreifer ohne Ihr Wissen auf Ihrem PC installiert werden.

Botnet: Böswilliges System, in dem mehrere Kopien eines Bots auf vielen PCs installiert sind und von einem böswilligen Hacker kontrolliert werden, der es für große Angriffe verwenden kann.

Steuerung und Kontrolle (Command and Control; C&C): Server und Infrastruktur, die verwendet werden, um viele Computer über zentralisierte Befehle zu steuern, wie etwa ein Botnet. Der Black Hat-Angreifer, der ein Botnet-C&C ausführt, wird als Botnet-Controller oder Botmaster bezeichnet.

Branchenprofil: Regierungsbehörden

Diese Regierungsbehörde hat fast alles richtig gemacht. Die Software wurde zeitnah gepatcht, eine relativ geringe Anzahl an Endbenutzern hat Administratorrechte und die routinemäßigen Sicherheitschecks (Prüfungen) wurden durchgeführt. Bonuspunkte gibt es für den Unterhalt dedizierter Arbeitsplätze für Administratoren für den Domänenadministrator und den Unternehmensadministrator. (Domänenadministratoren und Unternehmensadministratoren regulieren sämtliche anderen Konten in einem Unternehmen. Nur sehr wenige Personen in einem Unternehmen dürfen diese Zugangsebene haben. Das Zuweisen von Domänenadministratoren und Unternehmensadministratoren muss genau überwacht werden.)

Der fatale Fehler des Unternehmens: Dasselbe lokale Administratorkennwort wird im ganzen Unternehmen für Computer in Personalwesen, Buchhaltung und der kritischen IT-Verwaltung verwendet. Wie können gewandte Personen mit Regierungsressourcen einen derartigen Fehler begehen?

Die Verwendung gemeinsamer lokaler Administratorkennwörter ist eine standardmäßige Vorgehensweise in vielen Organisationen, die das Risiko nicht wahrnehmen. Gelegentlich funktioniert die anfängliche Einrichtung von Systemen mit eingeschränkten Konten nicht wie erwartet. Zur Behebung des Problems geben Administratoren diesen Konten mehr Rechte, bis die Anwendung funktioniert. Falls die Probleme nicht behoben sind, kann der Administrator die zusätzlichen Rechte als Problembehebung beibehalten. In anderen Situationen werden lokale Konten möglicherweise im Notfall verwendet und dann zur künftigen Verwendung auf dem System belassen. In jedem der Fälle ist das System für Angriffe offen. Diese IT-Verhaltensweisen offenbaren ein Sicherheitsbewusstsein, das nur auf lokaler Ebene vorhanden ist und keinen angemessenen Schutz in der Bedrohungsumgebung des stets aktiven und stets verbundenen Internets von heute darstellt.

Im Fall dieser Behörde konnte ein Angreifer in das Netzwerk gelangen, als ein Benutzer ein infiziertes Dokument aufgerufen oder auf einen Link zu einer Website geklickt hat, die schädlichen Code gehostet hat. (Der genaue Punkt der Infizierung ist nicht bekannt.) Da die Organisation dasselbe Administratorkennwort in allen Abteilungen verwendet hat, konnte der Angreifer das Netzwerk erkunden und alle Kennwörter von Domänenadmistratoren und Unternehmensadministratoren abrufen. Diese Anmeldeinformationen waren die "Schlüssel für das Königreich": Der Angreifer konnte Code in Rechenzentren, Server und Microsoft Exchange implantieren, was zu einer vollständigen Kompromittierung des Netzwerks mit Kosten in Höhe von Millionen von Dollar führte.

Die tatsächlichen Kosten des Angriffs, die das erneute Programmieren von Systemen, das erneute Ausstellen von Kennwörtern und öffentliche Untersuchungen von Datendiebstahl und Fehlern beinhalteten. Der Vertrauensverlust bei den Opfern des Angriffs lässt sich nicht in Zahlen ausdrücken.

Umfassende Verteidigungshaltung

Die Regierungsbehörde machte vieles richtig, es bedarf allerdings eines umfassenden Ansatzes, um einen Angriff erfolgreich abzuwehren.

Wir empfehlen die folgenden Abwehrmechanismen:

Microsoft Enhanced Mitigation Experience Toolkit (EMET): Dieses Hilfsprogramm dient der Verhinderung der Ausbeutung von Schwachstellen in der Software.

Microsoft Office 365: Diese Produktsuite soll die Sicherheitsanforderungen Ihres Unternehmens erfüllen, einschließlich Datennutzung mit juristischen, rechtlichen und technischen Standards.

Enhanced Security Administrative Environment (ESAE): Nutzt fortschrittliche Technologien und empfohlene Vorgehensweisen, um eine Administratorumgebung und Arbeitsplätze mit verbessertem Sicherheitsschutz bereitzustellen.

Privileged Identity Management for Active Directory: Ermöglicht Ihnen das Verwalten, Steuern und Überwachen Ihrer privilegierten Identitäten und deren Zugriff auf Ressourcen in Azure Active Directory sowie andere Microsoft-Onlinedienste (z. B. Office 365 und Microsoft Intune).

Microsoft Advanced Threat Analytics (ATA): Verwendet die Verhaltensanalyse zur Überwachung der anormalen Verwendung von Konten und Anmeldeinformationen.

Operations Management Suite (OMS): Cloud-basierte IT-Verwaltungslösung, mit der Sie einen Angreifer überwachen und nachverfolgen können.

Phase vier: Festsetzung für eine lange Persistenz

In Phase vier richtet sich der Angreifer langfristig ein, installiert getarnte dauerhafte Dienste, wie etwa Schadsoftware zur Ausnutzung von Schwachstellen und Überwachung und Extraktion von Daten, beim gleichzeitigen Versuch möglichst lange unerkannt zu bleiben. Angreifer erstellen Konten für sich selbst, um zu gewährleisten, dass sie im Netzwerk bleiben können und ändern Kennwörter, um unerkannt zu bleiben.

Wie in Phase drei verwenden Hacker Implantate oder Bots, um verschiedene Möglichkeiten zu schaffen, um in das Netzwerk zurück zu gelangen und sich in der Umgebung zu verstecken. Sie verwenden C&C, um ihren Fuß in der Tür zu halten, erkunden Ressourcen und rufennach Belieben Kanäle im ganzen Netzwerk auf. Wenn sie Verdacht hegen, dass sie entdeckt wurden, haben sie die Mittel und Ressourcen, um sich zu entfernen und den Zugang neu aufzubauen.

Gängige Begriffe: **Advanced Persistent Threat (APT):** Ein gezielter Angriff auf eine spezifische Entität, der versucht, ein Auffinden zu verhindern und Informationen über einen längeren Zeitraum zu stehlen.

Assume Breach: Eine strategische Denkweise. Für Führungskräfte und CISOs bedeutet es einen Wandel der Orientierung von rein präventiven Sicherheitsmaßnahmen hin zu Entdeckung, Reaktion und Erholung von Sicherheitsproblemen.

Branchenprofil: Hightech-Herstellung

Hacker können sehr, sehr geduldig sein. Nach der Infiltrierung eines Netzwerks können sie hunderte Tage unentdeckt bleiben. Während dieser Zeit programmieren sie Systeme um, überschreiben Protokolle und aktualisieren ihre Hackertools. Ein Hightech-Fertigungsunternehmen hatte bis zu seiner Entdeckung mindestens eineinhalb Jahre lang einen ungebetenen Gast in seinem Netzwerk. Während dieser Zeit implantierte der Angreifer fortschrittliche gezielte Schadsoftware auf dem Home Drive Server eines Kunden, der nahezu sämtliches geistiges Eigentum des Kunden beherbergte.

Die PowerPoint-Präsentationen, Dokumentation, Projektpläne und Fertigungsprozessdetails des Kunden standen dem Angreifer alle regelmäßig zur Verfügung. Eine enorme Menge an Forschungs- und Entwicklungsinformationen wurde aus verschiedenen Teilen des Kundennetzwerks gestohlen, bevor der Angriff entdeckt wurde.

Verbessern der Sicherheit

Niemand weiß, wie die Angreifer in das Kundennetzwerk des Herstellers gelangten. Basierend auf der Art des Angriffs wissen wir, dass die Angreifer eine Möglichkeit gefunden haben, sich selbst zu autorisieren, um die Schadsoftware installieren zu können.

Wir empfehlen die Verwendung der folgenden Tools, um diese Art des Angriffs zu verhindern:

Erweiterter Bedrohungsschutz: Dieses Feature in Office 365 scannt automatisch alle Anhänge und Links in eingehenden E-Mails auf potenzielle Bedrohungen. Fragwürdiges Material erreicht die Benutzer nicht. Dadurch werden die Social Engineering-Bedrohungen für Ihr Netzwerk reduziert.

Mehrstufige Autorisierung: Verlangt von Benutzern das Angeben zusätzlicher Verifizierungen über den Benutzernamen und das Kennwort hinaus. Beispiel: Einen Telefonanruf oder eine Textnachricht zur Bestätigung der Identität des Benutzers.

Azure Rights Management (Azure RMS): Diese Datenschutzlösung verwendet Verschlüsselungs-, Identitäts- und Autorisierungsrichtlinien, um Ihre Dateien und E-Mails zu schützen. Sie funktioniert auf mehreren Geräten, einschließlich Telefonen, Tablets und PCs.

Microsoft OneDrive: Diese Cloud-Speicherlösung bietet mehrere Möglichkeiten, um Dateien zu schützen. In OneDrive gespeicherte Dateien werden nie für andere Benutzer freigegeben, solange Sie sie nicht in einem öffentlichen Ordner aufbewahren oder bewusst freigeben möchten. Sie können die Sicherheit verbessern, indem Sie ein sicheres Kennwort erstellen, Sicherheitsmaßnahmen zu einem vorhandenen Microsoft-Konto hinzufügen (Beispiel: mit Ihrer alternativen E-Mail-Adresse oder einer Sicherheitsfrage) und die zweistufigen Verifizierung verwenden.

Microsoft Datacenter: Microsoft nutzt seine jahrzehntelange Erfahrung beim Erstellen von Unternehmenssoftware und Ausführen von globalen Onlinediensten zum Erstellen von Sicherheitstechnologien und -praktiken, denen Sie vertrauen können. Unsere Rechenzentren sind physisch aufgebaut, verwaltet und überwacht mit Zäunen, Wächtern, Prüfungen im Hintergrund, biometrischen Zugangskontrollen, Sicherheitsschulungen und dem Äquivalent eines Festplattenshredders zum Entsorgen von Servern. In allen Rechenzentren sind die 24-stündige Überwachung, mehrstufige Authentifizierung (einschließlich biometrisches Scannen) und ein internes Netzwerk vom öffentlichen Internet isoliert.

Branchenprofil: Internet-Einzelhandelsunternehmen

Unser letztes abschreckendes Beispiel stammt aus dem Internet.

Sie haben möglicherweise bereits von ein paar profilierten Angriffen auf Online-Einzelhändler gehört, bei denen der Angreifer nach Kundendaten für finanziellen Profit suchte. Online-Einzelhändler bieten in der Regel für die wichtigen Anbieter mit nur sehr wenigen Einschränkungen Remotenetzwerkzugang, wie etwa Kreditkartendienste. (In einigen Fällen bedeutet dies nahezu Zugriff auf Mitarbeiterebene.) Das ist die erste Warnung. Die zweite ist die fehlende Netzwerktrennung. In anderen Worten: Sobald jemand eingedrungen ist, kann er sich auf den gehackten Unternehmensservern frei bewegen.

Uns sind mehrere Fälle bekannt, bei denen Angreifer über ihre Anbieterverbindungen Remotezugriff auf die Server eines Zielunternehmens erhalten haben. Einmal im System, tarnt sich der Angreifer als Anbieter und erkundet die Systeme. Er versucht die wichtigsten zu knacken, die finanzielle Daten oder Konten enthalten, die auf derartige Daten zugreifen können. In anderen Worten hackten die Angreifer ein Unternehmen, um Zugriff auf ein weiteres Unternehmen zu erhalten, mit dem dieses Geschäfte tätigte.

Der Aktienkurs von auf diese Weise angegriffenen Einzelhändlern kann in nur einer Woche nach dem Angriff erheblich an Wert verlieren. Kompromittierte Unternehmen können auch von empfindlichen behördlichen Strafen getroffen werden, die bis in die Milliarden reichen – insbesondere in regulierten Branchen (mit Compliance-Anforderungen). Darüber hinaus können Strafen und Gerichtsverfahren gegen ein Unternehmen genutzt werden, das sich als schwaches Glied bei einem Angriff erwiesen hat. Einige Unternehmen verfügen über eine Versicherung für derartige Probleme mit Angriffen.

Einkaufsschutz

Der beste Weg, Hacker vom Angreifen über eine Remotezugriffsverbindung abzuhalten, ist das einfache Verbot des Remotezugriffs. Dies ist allerdings für viele Unternehmen nicht realistisch, wie etwa Onlinedienste und Einzelhandel.

Hier sind einige sicherere Möglichkeiten, die Anbietern den Zugriff auf Ihr Netzwerk ermöglichen:

Veröffentlichen über Azure: Verschieben Sie bestimmte interne Workloads, wie etwa Web-Schnittstellenzugriff und Back-End-Datenbanken auf eine vertrauenswürdige Cloud Platform-as-a-Service (PaaS). Die Cloud-Workload kann auf minimaler Zugriffsebene gehalten werden, damit sie nur die erforderlichen Daten im internen Netzwerk aufrufen kann. Diese Methode beschränkt die Anzahl der Benutzer mit direktem Zugriff auf ein Kundennetzwerk und reduziert die erforderlichen Rechte eines Benutzers innerhalb des Netzwerks, indem sie den Zugriff nur auf die erforderlichen PaaS-Ressourcen beschränkt.

Mehrstufige Autorisierung: Verlangt von Benutzern das Angeben zusätzlicher Verifizierungen über den Benutzernamen und das Kennwort hinaus. Beispiel: Einen Telefonanruf oder eine Textnachricht zur Bestätigung der Identität des Benutzers.

Migrieren Sie von einem Remote Desktop Connection (RDP)-Server auf virtuelle Computer (VMs) in Azure: Die Verwendung von VMs ermöglicht Ihnen das Pflegen eindeutiger Kennwörter für Netzwerksegmente und die Kontrolle des Zugriffs auf Informationen.

Schlussfolgerung

Schützen, Auffinden, Reagieren

Schützen, Auffinden, Reagieren

Bereit für eine Verbesserung Ihrer Unternehmenssicherheit? Wir empfehlen einen ganzheitlichen Ansatz. Sie müssen verstehen, wie gezielte Angriffe in der Regel erfolgen. Sie müssen erkennen, dass ein Angriff nur eine Frage der Zeit ist. Langfristige Kompromisse für Unternehmenssysteme werden regelmäßig geschlossen. Suchen Sie daher aktiv nach ihnen und ergreifen Sie Schritte, um diese zu lindern. Sie wissen, wie Sie effektiv und schnell auf einen gezielten Angriff reagieren.

Wir haben die Strategie in drei Schritte aufgeteilt:

Schritt eins: Schützen.
Verwenden Sie den Ansatz zur Risikoverwaltung mit den geringsten Rechten. Stellen Sie die folgenden Fragen:

- Muss diese Person wirklich darauf zugreifen können?
- Weiß ich, wo meine Daten sind?
- Weiß ich, wer Zugriff darauf hat?
- Weiß ich, wo bei Bedarf Konformität herrscht?
- Ist meine Software auf dem neuesten Stand?

Schritt zwei: Auffinden.
Nehmen Sie an, Sie werden angegriffen. Seien Sie misstrauisch. Stellen Sie die folgenden Fragen:

- Wie erfahre ich, wenn ein Angriff erfolgt ist?
- Habe ich die richtigen Tools, um einen Angriff zu erkennen?
- Habe ich die richtigen Tools, um einen Angriff zu analysieren?

Schritt drei: Reagieren.
Prüfen Sie, ob Sie einen Antwortprozess haben und ob darin die entsprechenden Auslöser eingerichtet sind. Stellen Sie die folgenden Fragen:

- Wie reagieren wir auf einen Angriff?
- Wie verwalten wir Schäden an Ressourcen und an unserem Ruf?
- Haben wir einen Kundenkommunikationsplan?
- Wie lernen wir daraus?

Microsoft ist bestrebt, Ihre Daten zu schützen und Ihre Systeme sicher und privat zu halten. Weitere Informationen über bewährte Vorgehensweisen für Cybersicherheit, Datenschutz und Kontrolle sowie Konformität in Ihrem Unternehmen finden Sie unter www.microsoft.com/trustedcloud.

Das Vertrauenswürdige Cloud-Team bedankt sich herzlich bei Bruce Cowper, Kasia Kaplinska, Matt Kemehar, IB Terry und Yvette Waters für ihre Zeit, ihr Wissen und Talent in der Entwicklung dieses E-Books.

© 2016 Microsoft Corporation. Alle Rechte vorbehalten. Dieses Dokument dient ausschließlich zu Informationszwecken. Microsoft gibt im Hinblick auf die hier präsentierten Informationen keine Garantieerklärungen ab, weder ausdrücklich noch stillschweigend.