Netzwerksicherheitsrichtlinie: Whitepaper zu Best Practices

Inhalt

Einführung

Ohne Sicherheitsrichtlinien kann die Verfügbarkeit Ihres Netzwerks beeinträchtigt werden. Die Richtlinie beginnt mit der Risikobewertung für das Netzwerk und dem Aufbau eines Teams zur Reaktion darauf. Die Fortsetzung der Richtlinie erfordert die Implementierung eines Verfahrens für das Management von Sicherheitsänderungen und die Überwachung des Netzwerks auf Sicherheitsverletzungen. Schließlich ändert der Überprüfungsprozess die bestehende Politik und passt sich den gewonnenen Erkenntnissen an.

Dieses Dokument ist in drei Bereiche unterteilt: Vorbereitung, Prävention und Reaktion. Schauen wir uns die einzelnen Schritte genauer an.

Vorbereitung

Sie müssen vor dem Implementieren einer Sicherheitsrichtlinie folgende Schritte ausführen:

- Erstellen Sie Nutzungsrichtlinienanweisungen.
- Führen Sie eine Risikoanalyse durch.
- Aufbau einer Sicherheitsteams-Struktur.

Erstellen von Nutzungsrichtlinien-Anweisungen

Es wird empfohlen, Nutzungsrichtlinien zu erstellen, in denen die Rollen und Verantwortlichkeiten

der Benutzer im Hinblick auf die Sicherheit beschrieben werden. Sie können mit einer allgemeinen Richtlinie beginnen, die alle Netzwerksysteme und -daten innerhalb Ihres Unternehmens abdeckt. Dieses Dokument sollte der allgemeinen Benutzer-Community ein Verständnis der Sicherheitsrichtlinien, ihres Zwecks, von Richtlinien zur Verbesserung ihrer Sicherheitsverfahren und von Definitionen ihrer Sicherheitsaufgaben vermitteln. Wenn Ihr Unternehmen spezifische Maßnahmen identifiziert hat, die zu strafrechtlichen oder disziplinarischen Maßnahmen gegen einen Mitarbeiter führen könnten, sollten diese Maßnahmen und deren Vermeidung in diesem Dokument klar dargelegt werden.

Der nächste Schritt besteht in der Erstellung einer Erklärung zur akzeptablen Nutzung für Partner, um Partnern ein Verständnis der Informationen zu vermitteln, die ihnen zur Verfügung stehen, die erwartete Einstufung dieser Informationen sowie das Verhalten der Mitarbeiter Ihres Unternehmens. Sie sollten genau erklären, welche konkreten Handlungen als Sicherheitsangriffe identifiziert wurden und welche Strafmaßnahmen ergriffen werden, wenn ein Sicherheitsangriff erkannt wird.

Erstellen Sie schließlich eine Administratoranweisung für akzeptable Nutzung, um die Verfahren für die Verwaltung von Benutzerkonten, die Richtliniendurchsetzung und die Überprüfung von Berechtigungen zu erläutern. Wenn Ihr Unternehmen spezifische Richtlinien bezüglich Benutzerkennwörtern oder der anschließenden Verarbeitung von Daten hat, stellen Sie diese auch klar dar. Überprüfen Sie die Richtlinie mit der akzeptablen Nutzung des Partners und den Richtlinien zur akzeptablen Nutzung, um Einheitlichkeit zu gewährleisten. Stellen Sie sicher, dass die in der Richtlinie für akzeptable Nutzung aufgeführten Administratoranforderungen in Schulungsplänen und Leistungsbewertungen berücksichtigt werden.

Durchführen einer Risikoanalyse

Eine Risikoanalyse sollte die Risiken für Ihr Netzwerk, Ihre Netzwerkressourcen und Ihre Daten identifizieren. Dies bedeutet nicht, dass Sie jeden möglichen Eintrittspunkt in das Netzwerk oder alle möglichen Angriffsmethoden identifizieren sollten. Ziel einer Risikoanalyse ist es, Teile Ihres Netzwerks zu identifizieren, jedem Teil eine Bedrohungsbewertung zuzuweisen und eine angemessene Sicherheitsstufe anzuwenden. So wird ein ausgewogenes Verhältnis zwischen Sicherheit und erforderlichem Netzwerkzugriff gewährleistet.

Weisen Sie jeder Netzwerkressource eine der folgenden drei Risikostufen zu:

- Systeme **mit geringem Risiko** oder Daten, die bei einer Kompromittierung (Anzeige von Daten durch unbefugtes Personal, beschädigte Daten oder verlorene Daten) das Geschäft nicht stören oder rechtliche oder finanzielle Auswirkungen haben. Das bzw. die Daten des Zielsystems können problemlos wiederhergestellt werden und ermöglichen keinen weiteren Zugriff auf andere Systeme.
- Systeme **mit mittlerem Risiko** oder Daten, die bei einer Kompromittierung (Anzeige von Daten durch unbefugtes Personal, beschädigte Daten oder verlorene Daten) eine mäßige Unterbrechung des Geschäftsbetriebs verursachen, geringfügige rechtliche oder finanzielle Auswirkungen haben oder weiteren Zugriff auf andere Systeme ermöglichen würden. Das Ziel-System oder die Zieldaten erfordern einen mäßigen Wiederherstellungsansatz, oder der Wiederherstellungsprozess führt zu einer Störung des Systems.
- Systeme **mit hohem Risiko** oder Daten, die bei einer Kompromittierung (Anzeige von Daten durch unbefugtes Personal, beschädigte Daten oder verlorene Daten) zu einer extremen Störung des Geschäftsbetriebs führen, erhebliche rechtliche oder finanzielle Auswirkungen haben oder die Gesundheit und Sicherheit einer Person gefährden würden. Das bzw. die

Zielsysteme oder Daten erfordern erhebliche Anstrengungen zur Wiederherstellung, oder der Wiederherstellungsprozess kann das Geschäft oder andere Systeme beeinträchtigen.

Weisen Sie jedem der folgenden Punkte eine Risikostufe zu: Core-Netzwerkgeräte, Verteilernetzwerkgeräte, Zugriffsnetzwerkgeräte, Netzwerküberwachungsgeräte (SNMP-Monitore und RMON-Probes), Netzwerksicherheitsgeräte (RADIUS und TACACS), E-Mail-Systeme, Netzwerkdateiserver, Netzwerkdruckserver, Netzwerkanwendungsserver (DNS und DHCP), Datenanwendungsserver (Oracle oder andere eigenständige Anwendungen), Desktop-Computer und andere Geräte (eigenständige Druckerserver und NetzwerkFaxgeräte).

Netzwerkgeräte wie Switches, Router, DNS-Server und DHCP-Server können einen weiteren Zugriff auf das Netzwerk ermöglichen und sind daher entweder Geräte mit mittlerem oder hohem Risiko. Es ist auch möglich, dass die Beschädigung dieser Geräte dazu führen kann, dass das Netzwerk selbst zusammenbricht. Ein solcher Ausfall kann das Geschäft extrem stören.

Sobald Sie eine Risikostufe zugewiesen haben, müssen Sie die Benutzertypen dieses Systems identifizieren. Die fünf häufigsten Benutzertypen sind:

- **Administratoren** Interne Benutzer, die für Netzwerkressourcen verantwortlich sind
- **Privilegierte** interne Benutzer, die einen besseren Zugriff benötigen.
- **Benutzer** Interne Benutzer mit allgemeinen Zugriffsrechten.
- **Partner** Externe Benutzer, die Zugriff auf bestimmte Ressourcen benötigen
- **Andere** externe Benutzer oder Kunden.

Die Ermittlung der Risikostufe und der erforderlichen Zugriffsart für die einzelnen Netzwerksysteme bildet die Grundlage der folgenden Sicherheitsmatrix. Die Sicherheitsmatrix bietet eine Kurzreferenz für jedes System und einen Ausgangspunkt für weitere Sicherheitsmaßnahmen, z. B. die Entwicklung einer geeigneten Strategie zur Beschränkung des Zugriffs auf Netzwerkressourcen.

System	Beschreibung	Risikostufe	Benutzertypen
ATM-Switches	Core-Netzwerkgerät	Hoch	Administratoren für die Gerätekonfiguration (nur Support-Mitarbeiter); Alle anderen für den Transport
Netzwerk-Router	Distribution-Netzwerkgerät	Hoch	Administratoren für die Gerätekonfiguration (nur Support-Mitarbeiter); Alle anderen für den Transport
Cloud-Switches	Netzwerkgerät aufrufen	Mittel	Administratoren für die Gerätekonfiguration (nur Support-Mitarbeiter); Alle anderen für den Transport
ISDN oder DFÜ-Server	Netzwerkgerät aufrufen	Mittel	Administratoren für die Gerätekonfiguration (nur Support-Mitarbeiter); Partner und privilegierte Benutzer für speziellen

			Zugriff
Firewall	Netzwerkgerät aufrufen	Hoch	Administratoren für die Gerätekonfiguration (nur Support-Mitarbeiter); Alle anderen für den Transport
DNS- und DHCP-Server	Netzwerkanwendungen	Mittel	Administratoren für die Konfiguration Allgemeine und privilegierte Benutzer zur Verwendung
Externer E-Mail-Server	Netzwerkanwendung	Niedrig	Administratoren für die Konfiguration Alle anderen für den E-Mail-Transport zwischen dem Internet und dem internen Mail-Server
Interner E-Mail-Server	Netzwerkanwendung	Mittel	Administratoren für die Konfiguration Alle anderen internen Benutzer
Oracle-Datenbank	Netzwerkanwendung	Mittel oder Hoch	Administratoren für die Systemverwaltung; Berechtigte Benutzer für Datenaktualisierungen; Allgemeine Benutzer für den Datenzugriff; Alle anderen für den partiellen Datenzugriff

Aufbau einer Sicherheitsteams-Struktur

Erstellen Sie ein funktionsübergreifendes Sicherheitsteam unter der Leitung eines Security Managers mit Teilnehmern aus den verschiedenen Geschäftsbereichen Ihres Unternehmens. Die Vertreter des Teams sollten sich der Sicherheitsrichtlinien und der technischen Aspekte des Sicherheitsdesigns und der Sicherheitsimplementierung bewusst sein. Dies erfordert häufig zusätzliche Schulungen für die Teammitglieder. Das Sicherheitsteam hat drei Verantwortungsbereiche: Entwicklung, Praxis und Reaktion von Richtlinien.

Die Entwicklung von Richtlinien konzentriert sich auf die Festlegung und Überprüfung von Sicherheitsrichtlinien für das Unternehmen. Überprüfen Sie mindestens einmal jährlich sowohl die Risikoanalyse als auch die Sicherheitsrichtlinie.

Die Praxis ist die Phase, in der das Sicherheitsteam die Risikoanalyse durchführt, Sicherheitsänderungsanträge genehmigt, Sicherheitswarnungen sowohl von Anbietern als auch von der CERT -Mailingliste prüft und rein sprachliche Sicherheitsrichtlinien in spezifische technische Implementierungen umwandelt.

Der letzte Verantwortungsbereich ist die Reaktion. Während die Netzwerküberwachung häufig eine Sicherheitsverletzung identifiziert, sind es die Mitglieder des Sicherheitsteams, die die eigentliche Fehlerbehebung und Behebung einer solchen Verletzung durchführen. Jedes

Sicherheitsteams sollte die Sicherheitsfunktionen der Geräte in seinem Betriebsbereich genau kennen.

Obwohl wir die Verantwortlichkeiten des gesamten Teams definiert haben, sollten Sie die individuellen Rollen und Verantwortlichkeiten der Mitglieder des Sicherheitsteams in Ihrer Sicherheitsrichtlinie definieren.

Prävention

Prävention kann in zwei Teile unterteilt werden: Genehmigung von Sicherheitsänderungen und Überwachung der Netzwerksicherheit.

Genehmigen von Sicherheitsänderungen

Sicherheitsänderungen werden als Änderungen an Netzwerkgeräten definiert, die sich möglicherweise auf die allgemeine Sicherheit des Netzwerks auswirken. Ihre Sicherheitsrichtlinie sollte spezifische Sicherheitskonfigurationsanforderungen in nicht-technischen Begriffen identifizieren. Anstatt also eine Anforderung als "Keine externen Quellen, für die FTP-Verbindungen über die Firewall zulässig sind" zu definieren, definieren Sie die Anforderung als "Externe Verbindungen sollten keine Dateien aus dem internen Netzwerk abrufen können". Sie müssen eine Reihe von Anforderungen für Ihr Unternehmen definieren.

Das Sicherheitsteam sollte die Liste der Anforderungen in einfacher Sprache überprüfen, um spezifische Probleme bei der Netzwerkkonfiguration oder dem Netzwerkdesign zu identifizieren, die den Anforderungen entsprechen. Sobald das Team die erforderlichen Netzwerkkonfigurationsänderungen zur Implementierung der Sicherheitsrichtlinie erstellt hat, können Sie diese auf zukünftige Konfigurationsänderungen anwenden. Das Sicherheitsteam kann zwar alle Änderungen überprüfen, aber bei diesem Prozess können nur Änderungen überprüft werden, die ein ausreichendes Risiko darstellen, um eine Sonderbehandlung zu rechtfertigen.

Wir empfehlen, dass das Sicherheitsteam die folgenden Änderungen überprüft:

- Alle Änderungen an der Firewall-Konfiguration.
- Alle Änderungen an Zugriffskontrolllisten (ACL).
- Alle Änderungen an der SNMP-Konfiguration (Simple Network Management Protocol).
- Jegliche Änderung oder Aktualisierung der Software, die sich von der Liste der genehmigten Softwareüberarbeitungen unterscheidet.

Wir empfehlen auch die Einhaltung der folgenden Richtlinien:

- routinemäßige Änderung von Passwörtern für Netzwerkgeräte
- Beschränken Sie den Zugriff auf Netzwerkgeräte auf eine genehmigte Personalliste.
- Stellen Sie sicher, dass die aktuellen Software-Revisionsstufen für Netzwerkgeräte und Serverumgebungen den Sicherheitskonfigurationsanforderungen entsprechen.

Zusätzlich zu diesen Genehmigungsrichtlinien sollte ein Vertreter des Sicherheitsteams im Change Management Approval Board sitzen, um alle Änderungen zu überwachen, die das Board prüft. Der Vertreter des Sicherheitsteams kann jede Änderung, die als Sicherheitsänderung gilt, ablehnen, bis sie vom Sicherheitsteam genehmigt wurde.

Überwachen der Sicherheit Ihres Netzwerks

Die Sicherheitsüberwachung ähnelt der Netzwerküberwachung, allerdings konzentriert sie sich auf die Erkennung von Netzwerkänderungen, die auf eine Sicherheitsverletzung hinweisen. Der Ausgangspunkt für die Sicherheitsüberwachung ist die Feststellung einer Verletzung. Im Rahmen einer Risikoanalyse haben wir den erforderlichen Grad der Überwachung ermittelt, basierend auf der Bedrohung für das System. Bei der Genehmigung von Sicherheitsänderungen haben wir spezifische Bedrohungen für das Netzwerk identifiziert. Wenn wir uns diese beiden Parameter anschauen, entwickeln wir ein klares Bild davon, was Sie überwachen müssen und wie oft.

In der Risikoanalysematrix wird die Firewall als Netzwerkgerät mit hohem Risiko angesehen, was bedeutet, dass Sie sie in Echtzeit überwachen sollten. Im Abschnitt Genehmigen von Sicherheitsänderungen sehen Sie, dass Sie alle Änderungen an der Firewall überwachen sollten. Das bedeutet, dass der SNMP-Polling-Agent Vorgänge wie fehlgeschlagene Anmeldeversuche, ungewöhnlicher Datenverkehr, Änderungen an der Firewall, der Zugriff auf die Firewall und die Einrichtung von Verbindungen über die Firewall überwachen sollte.

Erstellen Sie im Anschluss an dieses Beispiel eine Überwachungsrichtlinie für jeden in Ihrer Risikoanalyse identifizierten Bereich. Wir empfehlen, Geräte mit geringem Risiko wöchentlich, Geräte mit mittlerem Risiko täglich und Geräte mit hohem Risiko stündlich zu überwachen. Wenn Sie eine schnellere Erkennung benötigen, sollten Sie diese in kürzerer Zeit überwachen.

Schließlich sollten Ihre Sicherheitsrichtlinien festlegen, wie das Sicherheitsteam über Sicherheitsverletzungen benachrichtigt werden soll. In vielen Fällen wird Ihre Netzwerküberwachungssoftware als erste die Verletzung erkennen. Es sollte eine Benachrichtigung an die Einsatzzentrale auslösen, die wiederum das Sicherheitsteam benachrichtigen sollte, falls erforderlich, indem ein Pager verwendet wird.

Antwort

Die Antwort kann in drei Teile unterteilt werden: Sicherheitsverletzungen, Wiederherstellung und Überprüfung.

Sicherheitsverletzungen

Wenn eine Verletzung erkannt wird, hängt die Fähigkeit zum Schutz der Netzwerkgeräte, zur Ermittlung des Angriffs und zur Wiederherstellung normaler Abläufe von schnellen Entscheidungen ab. Wenn diese Entscheidungen im Voraus getroffen werden, ist die Reaktion auf einen Eindringling viel leichter zu bewältigen.

Die erste Aktion nach der Erkennung eines Eindringlings ist die Benachrichtigung des Sicherheitsteams. Ohne ein Verfahren wird es erhebliche Verzögerungen geben, wenn die richtigen Personen die richtige Antwort erhalten. Definieren Sie ein Verfahren in Ihrer Sicherheitsrichtlinie, das rund um die Uhr, 7 Tage die Woche, verfügbar ist.

Als Nächstes sollten Sie festlegen, wie weit das Sicherheitsteam für Änderungen zuständig ist und in welcher Reihenfolge diese vorgenommen werden sollen. Mögliche Korrekturmaßnahmen sind:

- Implementieren von Änderungen, um den weiteren Zugriff auf die Verletzung zu verhindern.
- Isolierung der verletzten Systeme.
- Kontaktieren Sie den Carrier oder ISP, um den Angriff nachzuverfolgen.
- Verwenden von Aufzeichnungsgeräten zum Erfassen von Beweisen.
- Trennung verletzter Systeme oder Quelle der Verletzung.

- Kontaktaufnahme mit der Polizei oder anderen Regierungsbehörden.
- Herunterfahren verletzter Systeme.
- Wiederherstellung von Systemen nach einer priorisierten Liste.
- Benachrichtigung des internen leitenden und juristischen Personals

Stellen Sie sicher, dass alle Änderungen, die ohne Genehmigung durch das Management durchgeführt werden können, in der Sicherheitsrichtlinie detailliert beschrieben werden.

Außerdem gibt es zwei Gründe für das Erfassen und Pflegen von Informationen während eines Sicherheitsangriffs: um festzustellen, in welchem Umfang Systeme durch einen Sicherheitsangriff kompromittiert wurden, und um externe Verstöße zu verfolgen. Die Art der Informationen und die Art und Weise, wie Sie sie sammeln, hängt von Ihrem Ziel ab.

Gehen Sie wie folgt vor, um das Ausmaß der Verletzung zu ermitteln:

- Zeichnen Sie das Ereignis auf, indem Sie Sniffer-Traces für das Netzwerk, Kopien von Protokolldateien, aktive Benutzerkonten und Netzwerkverbindungen abrufen.
- Schränken Sie weitere Kompromittierungen ein, indem Sie Konten deaktivieren, Netzwerkgeräte vom Netzwerk trennen und die Verbindung zum Internet trennen.
- Sichern Sie das kompromittierte System, um eine detaillierte Analyse des Schadens und der Angriffsmethode zu unterstützen.
- Suchen Sie nach weiteren Anzeichen der Kompromittierung. Häufig sind andere Systeme oder Konten betroffen, wenn ein System kompromittiert wird.
- Verwalten und Überprüfen von Protokolldateien von Sicherheitsgeräten und Protokolldateien der Netzwerküberwachung, da diese häufig Hinweise auf die Angriffsmethode enthalten.

Wenn Sie gerichtlich tätig werden möchten, lassen Sie Ihre Rechtsabteilung die Verfahren zur Erfassung von Beweismitteln und zur Beteiligung der Behörden überprüfen. Eine solche Überprüfung erhöht die Wirksamkeit der Beweismittel in Gerichtsverfahren. Wenn die Verletzung in der Natur war, wenden Sie sich an Ihre Personalabteilung.

Wiederherstellung

Die Wiederherstellung des normalen Netzwerkbetriebs ist das Endziel jeder Reaktion auf Sicherheitsverletzungen. Legen Sie in den Sicherheitsrichtlinien fest, wie Sie normale Backups durchführen, sichern und verfügbar machen. Da jedes System über eigene Mittel und Verfahren für die Sicherung verfügt, sollte die Sicherheitsrichtlinie als Meta-Richtlinie fungieren, in der für jedes System die Sicherheitsbedingungen angegeben werden, die eine Wiederherstellung aus dem Backup erfordern. Wenn eine Wiederherstellung erst nach Genehmigung durchgeführt werden kann, müssen Sie auch den Prozess zur Genehmigung angeben.

Überprüfen

Der Überprüfungsprozess ist der letzte Schritt bei der Erstellung und Pflege von Sicherheitsrichtlinien. Es gibt drei Punkte, die Sie überprüfen müssen: Richtlinien, Haltung und Praxis.

Die Sicherheitsrichtlinien sollten ein lebendiges Dokument sein, das sich an eine sich ständig verändernde Umgebung anpasst. Durch die Überprüfung der bestehenden Richtlinie anhand bekannter Best Practices bleibt das Netzwerk auf dem neuesten Stand. Auf der CERT-Website finden Sie nützliche Tipps, Vorgehensweisen, Sicherheitsverbesserungen und Warnmeldungen, die Sie in Ihre Sicherheitsrichtlinien integrieren können.

Sie sollten auch den Status des Netzwerks im Vergleich zum gewünschten Sicherheitsstatus überprüfen. Ein auf Sicherheit spezialisiertes externes Unternehmen kann versuchen, in das Netzwerk einzudringen und nicht nur den Netzwerkstatus, sondern auch die Sicherheitsreaktion Ihres Unternehmens zu testen. Für Netzwerke mit hoher Verfügbarkeit empfehlen wir, diesen Test jährlich durchzuführen.

Schließlich wird die Praxis als Übung oder Test der Support-Mitarbeiter definiert, um sicherzustellen, dass sie eine klare Vorstellung davon haben, was sie bei einer Sicherheitsverletzung tun müssen. Häufig wird diese Übung vom Management unangekündigt und in Verbindung mit dem Netzwerkstatustest durchgeführt. Bei dieser Überprüfung werden Verfahrenslücken und Lücken bei der Personalausbildung aufgezeigt, sodass Abhilfemaßnahmen ergriffen werden können.

Zugehörige Informationen

- Weitere Whitepaper zu Best Practices
- Technischer Support – Cisco Systems