Oktober 2021

Bezahlen Sie kein Lösegeld

Eine dreistufige Anleitung zum Schutz vor Ransomware

Barracuda
Your journey, secured.

Inhaltsverzeichnis

Ransomware und ihre Weiterentwicklungen 1

Cyberkriminelle erhöhen den Einsatz 3

1. Schritt: Schützen Sie Ihre Zugangsdaten 5

Detection-and-Response-Tools 7

Schulung Ihrer Benutzer 8

2. Schritt: Schützen Sie Ihre Web-Applikationen und den Zugriff darauf 9

Vier Angriffsvektoren für Web-Applikationen 12

Wie ein Ransomware-Angriff Schwachstellen in Applikationen ausnutzt 15

So sichern Sie Ihre Applikationen und den Zugriff darauf 18

3. Schritt: Sichern Sie Ihre Daten 21

Was benötigen Sie in einer Backup-Lösung? 25

Fazit 26

Seien Sie darauf vorbereitet, auf einen Angriff zu reagieren 27

Bleiben Sie auf dem Laufenden 28

Barracuda

Ransomware und ihre Weiterentwicklungen

Einfach ausgedrückt: Ransomware ist eine bösartige Software, die Ihre Daten entweder verschlüsselt oder Sie anderweitig daran hindert, auf Ihre eigenen Systeme zuzugreifen. Die Kriminellen verlangen anschließend Lösegeld im Austausch für den Entschlüsselungscode. Natürlich gibt es keine Garantie dafür, dass der Code funktioniert und Sie Ihre Daten zurückbekommen. Viele Opfer haben ihre Daten trotz Bezahlung nicht zurückbekommen.

Im Vergleich zu den unkomplizierten WannaCry-Angriffen im Stil von „Kompromittieren und Verschlüsseln“ vor einigen Jahren verfolgen die Angreifer heute einen ausgefeilteren Multi-Vektor-Ansatz. Die Angriffe beginnen zwar immer noch häufig mit einer Spear-Phishing-E-Mail, aber die heutigen Ransomware-Angriffe werden nicht sofort ausgelöst, wenn die Zielperson auf den bösartigen Link klickt.

Stattdessen nutzen Cyberkriminelle diesen Schritt nun, um die Zugangsdaten ihrer Opfer zu stehlen. Mithilfe dieser Zugangsdaten greifen sie dann auf das Netzwerk des Unternehmens zu, wo sie ihren Opfern weiter auflauern und sich einen Überblick über deren Assets, Server, Datenbanken und E-Mail-Plattform verschaffen. Diese Beobachtungsphase kann sich über Wochen oder sogar Monate erstrecken, bevor sie ihren Angriff starten. Genau dieses Vorgehen konnte auch beim jüngsten Ransomware-Angriff auf die irische Gesundheitsbehörde HSE beobachtet werden. Die Angreifer behaupten, dass sie sich wochenlang im HSE-Netzwerk aufgehalten hatten, bevor sie den Angriff starteten, bei dem ganze 700 GB an Patientendaten verschlüsselt und gestohlen wurden.

Man hört momentan auch deshalb öfters etwas über Ransomware, weil die Einstiegsbarrieren weggefallen sind. Die Technologien, mit denen Verbrechen begangen werden, sind immer einfacher zu handhaben. Inzwischen kann man sich ein Ransomware-Kit kaufen und sein Ziel auswählen. Im Tausch gegen einen Prozentsatz des Lösegelds bieten Banden technische Unterstützung an. Wenn das zu abschreckend ist, können potenzielle Kriminelle Cyberkriminelle anheuern, die den Angriff für sie im Rahmen einer Cybercrime-as-a-Service-Vereinbarung durchführen. Der Wertzuwachs von Kryptowährungen und die Beliebtheit von Cyber-Versicherungen haben Ransomware-Angriffe für Cyber-Kriminelle profitabler gemacht und locken bestens organisierte Banden an. Außerdem haben staatlich finanzierte Ransomware-Angriffe die Cyber-Kriegsführung auf ein neues Niveau gehoben.

Barracuda

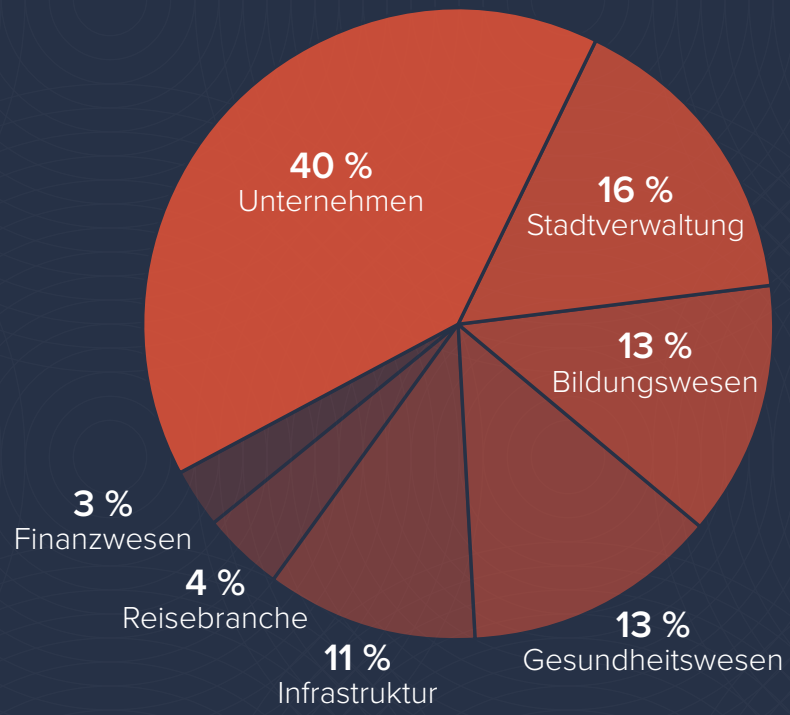
Cyberkriminelle erhöhen den Einsatz

Ransomware-Angriffe sind so weit eskaliert, dass Regierungen sie nun als terroristische Handlungen einstufen. Diese Reaktion ist alles andere als übertrieben. Diese Angriffe haben zu massiven Betriebsstörungen bei Kommunalverwaltungen, Strafverfolgungsbehörden, Bildungseinrichtungen, Gesundheitsnetzwerken, kritischen Infrastrukturen und anderen Bereichen geführt. Keine Branche, Organisation oder staatliche Einrichtung ist gegen diese Angriffe immun.

Laut aktuellen Untersuchungen von Barracuda machten Angriffe auf Infrastruktur-, Reise-, Finanzdienstleistungs- und andere Unternehmen zwischen August 2020 und Juli 2021 57 % aller Ransomware-Angriffe aus, gegenüber nur 18 % in unserer Studie aus dem Jahr 2020. Auf Infrastruktur-Unternehmen entfielen 11 % aller untersuchten Angriffe.

Auch die Lösegeldsummen steigen dramatisch an, sodass die durchschnittliche Lösegeldforderung pro Vorfall inzwischen bei über 10 Millionen Dollar liegt. Nur bei 18 % der von Barracuda zwischen August 2020 und Juli 2021 analysierten Vorfälle ging es um Lösegeldforderungen von weniger als 10 Millionen US-Dollar. Bei 30 % der Vorfälle ging es um Lösegeldforderungen von mehr als 30 Millionen US-Dollar.

Ransomware-Angriffe nach Branchen



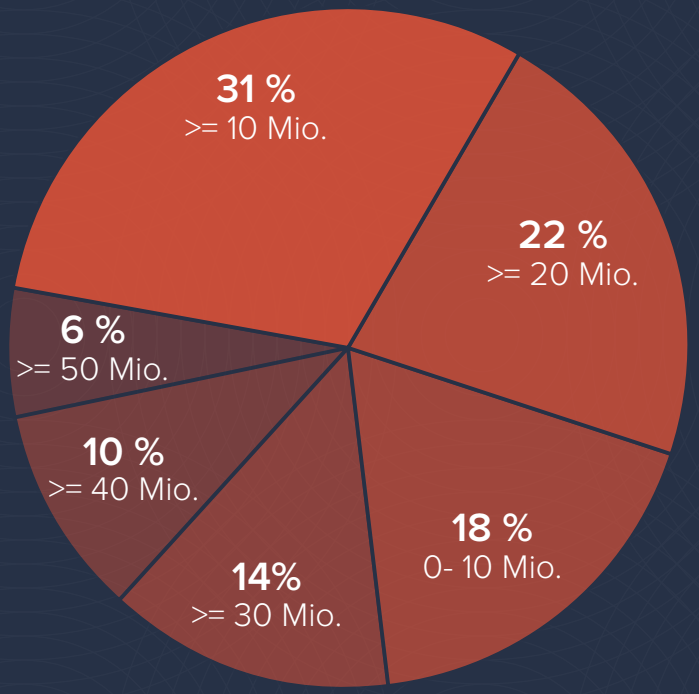
Ransomware ist keine neue Bedrohung, doch sie hat im Laufe der Zeit zerstörerische Ausmaße angenommen. Die Kriminellen, die dahinterstehen, haben ihre Fähigkeiten erweitert und ihre Taktiken verfeinert – einige von ihnen setzen auf Angriffe mit doppelter Erpressung. Ihre Lösegeldforderungen betreffen Informationen, die sie vor dem eigentlichen Verschlüsselungsangriff erfassen. Sie stehlen sensible Daten und verlangen im Austausch für das Versprechen, die Daten nicht zu veröffentlichen oder an andere Kriminelle zu verkaufen, die Zahlung einer Geldsumme. Natürlich gibt es für die Opfer keine Garantie, dass die Angreifer diese Versprechen halten. Oft werden die Betroffenen einige Monate nach erfolgter Lösegeldzahlung erneut kontaktiert und dazu genötigt, eine weitere Auszahlung vorzunehmen, damit die entwendeten Daten nicht weitergegeben werden. Einige Ransomware-Kriminelle geben die Daten trotz erfolgter Zahlung weiter.

Es gibt auch keine Garantie dafür, dass die verschlüsselten Daten nach einer Lösegeldzahlung wieder freigegeben werden. Die Opfer von Ransomware-Angriffen müssen sich daher bewusst sein, dass ihre gestohlenen Daten für immer kompromittiert bleiben werden. Folglich gibt es absolut keinen Grund, auf die Bedingungen der Kriminellen einzugehen.

Sie sollten davon ausgehen, dass es zu Ransomware-Angriffen auf Ihr Unternehmen kommen wird. Wenn der Angriff erfolgreich ist, sollten Sie einen Plan B haben, um das Lösegeld nicht zahlen zu müssen.

Eine effektive Abwehr von Ransomware-Angriffen besteht ganz einfach darin, die Daten Ihres Unternehmens zu schützen. Sie können dies in drei Schwerpunktbereiche unterteilen: Schutz Ihrer Zugangsdaten, Sicherung Ihrer Web-Applikationen und Sicherung Ihrer Daten. Nehmen wir uns jeden dieser Schritte genauer vor.

Ransomware-Forderungen



1. Schritt: Schützen Sie Ihre Zugangsdaten

Zunächst einmal beruht Ransomware darauf, dass entweder E-Mails geknackt oder Zugangsdaten anderweitig beschafft werden. Bei Zehntausenden von Benutzernamen und Passwörtern, die online leicht verfügbar sind, kann dieser erste Schritt erschreckend einfach sein. Angreifer verwenden dann diese gestohlenen Zugangsdaten für den Zugriff auf Ihre Systeme.

Barracuda

Da Phishing der primäre Angriffsvektor für Ransomware ist, müssen Sie eine Kultur des Risikobewusstseins für die Sicherheit von Zugangsdaten aufrechterhalten. Entwickeln Sie einen Prozess, um Benutzer in der E-Mail-Sicherheit zu schulen und setzen Sie Anti-Phishing-Technologie ein, die ungewöhnliche Aktivitäten identifizieren und melden kann. Wenn der Angreifer auf keine Zugangsdaten zugreifen kann, ist es viel schwieriger, den Angriff von Phishing auf Ransomware zu verschärfen.

Phishing-Angriffe funktionieren, weil Menschen Dinge einfach gerne anklicken. Hacker können Angriffe sorgfältig auf ihre Opfer zuschneiden, indem sie öffentlich verfügbare persönliche Informationen über sie sammeln und eine umgehende Antwort auf dringlich klingende Anliegen fordern. Den Angreifern reicht es, wenn nur eine Person in Ihrem Unternehmen auf den Link klickt oder einen Anhang öffnet. Jüngste Untersuchungen von Barracuda haben ergeben, dass im Durchschnitt 3 % der Personen, die eine Phishing-E-Mail erhalten, auf den Link klicken. Ziel des Angriffs ist es in der Regel, Zugangsdaten zu erbeuten, die es dem Hacker ermöglichen, sich im Unternehmen auszubreiten und das gesamte Unternehmen zu erpressen.

Geschützte Zugangsdaten und Zugriffe erfordern einen zweigleisigen Ansatz: Investieren Sie zunächst in Erkennungs- und Reaktionstools und konzentrieren Sie sich dann auf die Schulung Ihrer Benutzer.

2,94 %
KLICKEN LINK IN BÖSARTIGER E-MAIL AN

0,78 %
LEITEN BÖSARTIGE E-MAILS WEITER

0,17 %
ANTWORTEN AUF BÖSARTIGE E-MAIL

Quelle: Threat Spotlight: E-Mail-Bedrohungen nach der Zustellung

Barracuda

Detection-and-Response-Tools

Ihre E-Mail-Schutz-Technologie sollte sich nicht nur auf die Erkennung bösartiger Payloads konzentrieren, die über Links oder Anhänge zugestellt werden, sondern auch erkennen, wenn Angreifer Social-Engineering-Taktiken einsetzen, um Filtertechnologien zu umgehen und Benutzer zu Aktionen zu verleiten. Sie sollte in einer E-Mail nach einer bösartigen Absicht suchen, selbst wenn sie keine bösartige Payload enthält. Die E-Mail-Sicherheit, die Algorithmen des maschinellen Lernens nutzt, kann Social-Engineering-Angriffe durch die Suche nach kleinsten Abweichungen von üblichen Kommunikationsmustern mit höherer Genauigkeit erkennen.

Der Schutz der Zugangsdaten Ihrer Benutzer kann ohne ordnungsgemäßen Schutz vor einem Account Takeover nicht durchgeführt werden. Die Multifaktor-Authentifizierung (MFA) ist nach wie vor Best Practice und sollte heute von jedem Unternehmen angewendet werden. Sie ist jedoch keine Wunderwaffe und reicht leider nicht immer aus. Hacker versuchen, Möglichkeiten zur Umgehung der MFA zu finden, indem sie Benutzer entweder dazu bringen, Malware auf ihren Verifizierungsgeräten zu installieren oder gefälschten Apps Zugriff auf ihre Konten zu gewähren. Unternehmen müssen einen Schutz vor Account Takeover einrichten, der bösartige Aktivitäten wie verdächtige Log-ins oder Angriffe, die von kompromittierten Konten aus gestartet werden, schnell erkennt und Alarm schlägt.

Geschützte Zugangsdaten und Zugriffe erfordern einen zweigleisigen Ansatz: Investieren Sie zunächst in Erkennungs- und Reaktionstools und konzentrieren Sie sich dann auf die Schulung Ihrer Benutzer.

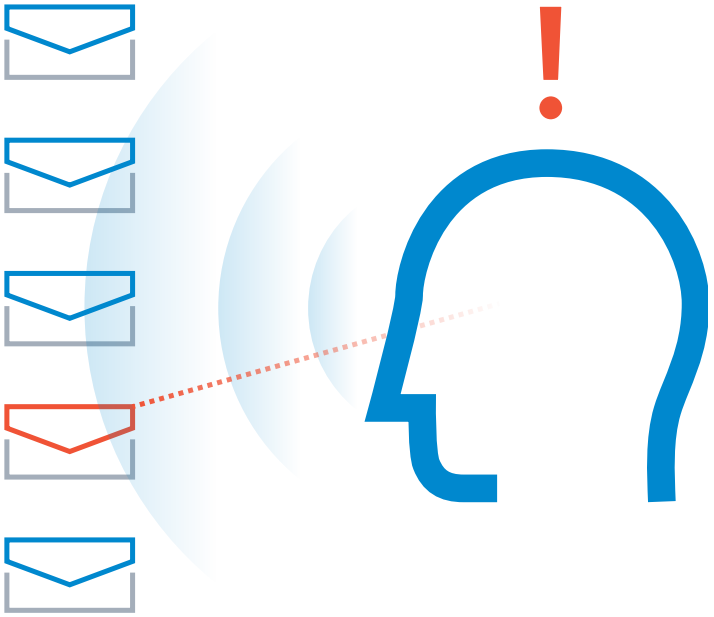
Barracuda

Schulung Ihrer Benutzer

Schlussendlich ist es entscheidend, Ihre Mitarbeiter im Erkennen und Melden von Angriffen zu schulen. Schulungen zur Stärkung des Risikobewusstseins und Phishing-Simulationen müssen Teil Ihrer Strategie zur E-Mail-Sicherheit sein. In der Vergangenheit wurden Phishing-Angriffe ausschließlich mit E-Mails in Verbindung gebracht, doch heute nutzen Cyberkriminelle auch andere Kanäle wie SMS und Sprachnachrichten. Verwenden Sie Phishing-Simulationen für E-Mails, Voicemail und SMS, um Benutzer im Erkennen von Cyberangriffen zu schulen, um die Wirksamkeit Ihrer Schulungen zu testen und die Benutzer zu identifizieren, die am anfälligsten für Angriffe sind.

Stellen Sie sicher, dass Cybersicherheitsschulungen nicht nur Teil der Einarbeitung für neue Mitarbeiter sind. Sämtliche Mitarbeiter müssen über die Entwicklung von Bedrohungen auf dem Laufenden gehalten werden. Zum Beispiel nutzen die kriminellen Gruppen heutzutage fortschrittliches Social Engineering, das schwer zu erkennen ist. Spear-Phishing-Angriffe zielen mit äußerst maßgeschneiderten Nachrichten auf eine einzelne Person oder einen Teil einer Abteilung, wie z. B. der Finanzabteilung, ab.

Entscheidend ist, dass Ihre Mitarbeiter durch die Schulungen Vertrauen gewinnen und es wagen, Alarm zu schlagen, selbst wenn es sich um einen Fehler handelt, den sie versehentlich verursacht haben. Möglicherweise ist eine Nachschulung erforderlich, aber Sie sollten Mitarbeiter, die eine Meldung machen, nicht bestrafen. Viele Angriffe werden nicht gemeldet, weil die Mitarbeiter befürchten, dass sie für das Anklicken eines Links oder das Öffnen eines Anhangs getadelt werden könnten. Zeitnahe Meldungen sind äußerst wertvoll und sollten gelobt werden.



2. Schritt: Schützen Sie Ihre Web-Applikationen und den Zugriff darauf

Der Wechsel zum externen Arbeiten hat noch mehr Applikationen aus dem Rechenzentrum ins Internet übertragen. Manchmal wurde in der Eile, den Betrieb von Unternehmensdiensten aufrechtzuerhalten, die Sicherheit vernachlässigt, und Cyberkriminelle sind bereit, diese Schwachstellen auszunutzen.

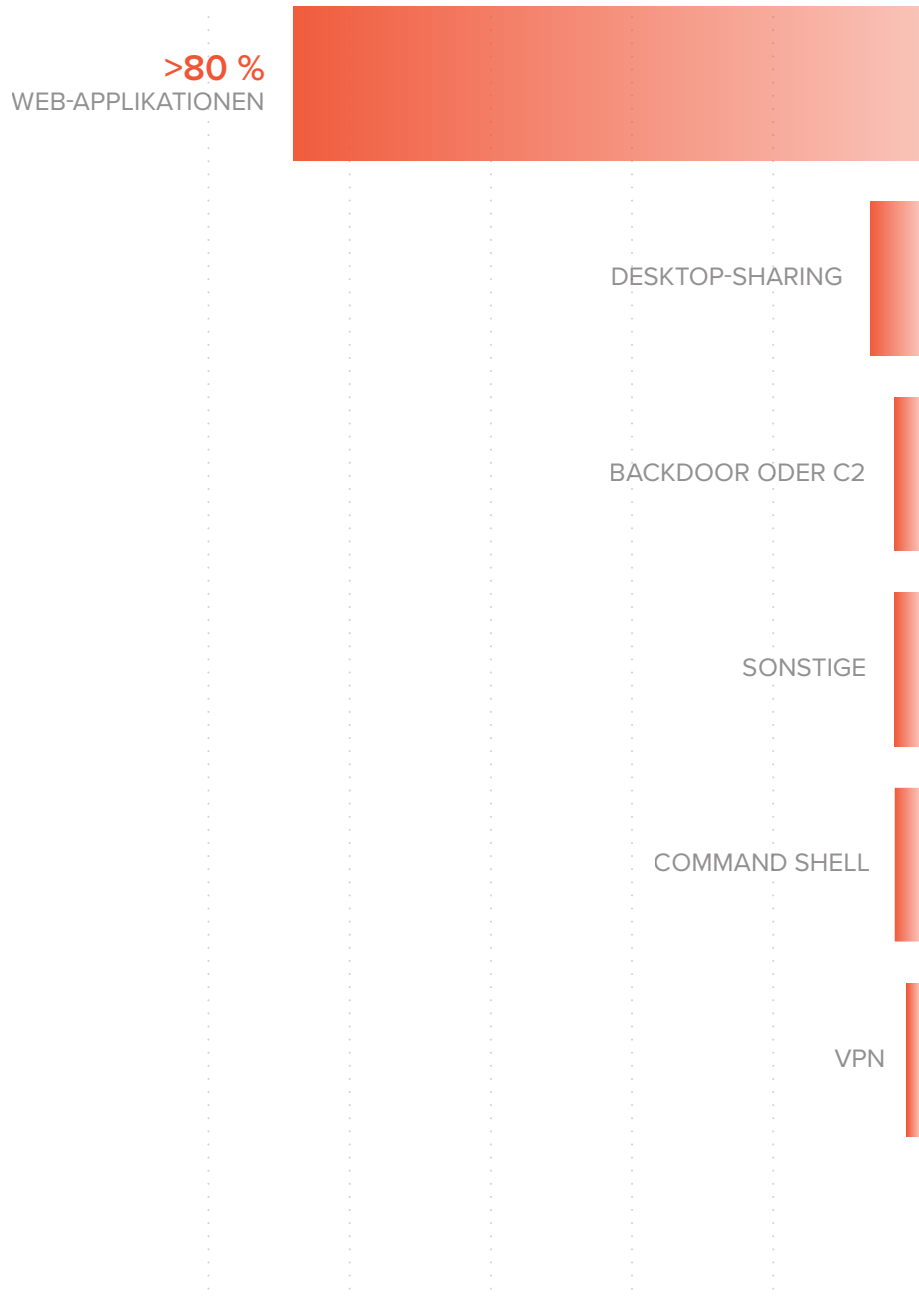
Barracuda

Gemäß dem Verizon Data Breach Investigations Report 2021 stellen Web-Applikationen den größten Angriffsvektor für Hacker dar und sind für mehr als 80 Prozent aller Datenschutzverletzungen verantwortlich.

Online-Applikationen wie File-Sharing-Dienste, Webformulare und E-Commerce-Websites können von Angreifern kompromittiert werden. Web-Applikationen werden über die Benutzeroberfläche oder eine API-Schnittstelle angegriffen. Oft umfassen diese Angriffe Credential Stuffing, Brute-Force-Angriffe oder OWASP-Schwachstellen. Sobald die Anwendung kompromittiert wurde, kann der Angreifer Ransomware und andere Malware in das System einschleusen. Diese kann sich dann lateral ausbreiten und Ihr Unternehmensnetzwerk sowie das der Anwendungsnutzer weiter infizieren.

Wenn es um den Schutz vor Ransomware und anderer Malware geht, sind der Schutz von Anwendungen und der Zugriffsschutz genauso wichtig wie die E-Mail-Sicherheit. Das Open Web Application Security Project (OWASP) hat zum Ziel, das öffentliche Bewusstsein für die häufigsten Schwachstellen zu schärfen, die bei einem Ransomware-Angriff ausgenutzt werden können.

Quelle: Verizon Data Breach Investigations Report 2021



Ein aktuelles Beispiel ist der REvil Ransomware Supply Chain Hack, der im Juli 2021 ans Licht kam. Schwachstellen in einer öffentlich zugänglichen Internet-MSP-Anwendung wurden ausgenutzt, um Ransomware an ihre Kunden zu verbreiten. In diesem Fall konnte sich die Ransomware aufgrund der tiefgreifenden Berechtigungen recht einfach ausbreiten und erheblichen Schaden anrichten, bevor sie gestoppt wurde. Alle mit dem Internet verbundenen Anwendungen sind anfällig für diese Art von Angriff. Angreifer verschaffen sich Zugang zur Anwendung und bewegen sich dann lateral, um Chaos anzurichten. Ein ähnliches Szenario kann auftreten, wenn man RDP-Systeme für das Internet offen lässt – auch dann, wenn man den Standardport ändert, denn Angreifer setzen gestohlene Zugangsdaten ein, um das gesamte Netzwerk über diesen ungeschützten Angriffsvektor mit Ransomware zu infizieren.

Bis zu

1500

Unternehmen sind von „REvil Supply Chain“-Angriffen betroffen

Barracuda.

Vier Angriffsvektoren für Web-Applikationen

Da Anwendungen mittlerweile ein beliebtes Ziel für Ransomware sind, gibt es vier Angriffsvektoren, die Sie schützen müssen: Anwendungszugriff, Schwachstellen in Web-Applikationen, Infrastruktur-Zugriff und laterale Bewegungen.

1. Zugriff auf die Applikation

Um festzustellen, ob der Anwendungszugriff ein Problem für Ihr Unternehmen darstellen könnte, müssen Sie einige wichtige Fragen beantworten.

- **Verwenden Ihre externen Mitarbeiter oder Vertragsarbeiter nicht verwaltete Geräte oder „Bring Your Own Device (BYOD)“?** Das trifft am häufigsten auf mobile Geräte zu. Ein nicht verwaltetes oder BYOD-Gerät kann kompromittiert und dann zum Extrahieren von Zugangsdaten oder für weitere Angriffe auf Ihre Applikation verwendet werden.
- **Haben Sie Einblick in alle Benutzer und Geräte im Netzwerk?** Sie müssen zum Beispiel wissen, wer sich mit Ihrem Gastnetzwerk verbindet und ob es richtig segmentiert ist.
- **Haben Sie einen Audit-Trail dafür, wer wann auf was zugreift?** Sie sollten zurückverfolgen können, wer auf Ihre Anwendungen zugreift, wie der Zugriff aussieht und ob die richtigen Berechtigungen vorlagen.

Wenn ein Gerät, das nicht für das Netzwerk zugelassen ist, mit Ihrem Netzwerk verbunden ist und jemand darauf ein Hacking-Tool eingerichtet hat, ist das ein ernstzunehmendes Problem. Und wenn Sie keinen Einblick in all dies haben, wird es schwierig zu erkennen, wer auf was zugreift und wo sich die Schwachstelle befindet. Sie werden also nicht in der Lage sein, die Sicherheitslücke zu schließen oder den Zugang des Angreifers zu blockieren.

2. Schwachstellen von Web-Applikationen

Schwachstellen in Web-Applikationen sind der nächste Angriffsvektor, den es zu bewerten gilt, wenn Sie die Sicherheit Ihrer Applikationen bewerten wollen.

Stellen Sie sich die folgenden Fragen:

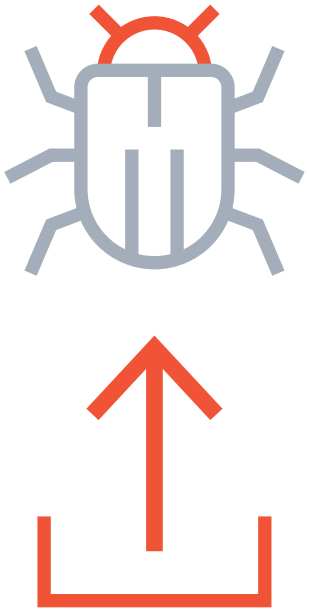
- Wie sicher ist Ihre Website? Wann wurde sie zuletzt aktualisiert?
- Haben Sie Formulare auf Ihrer Website? Wie verhindern Sie Angriffe durch Formulare?
- Können auf Ihrer Website Dateien hochgeladen werden? Wie schützen Sie sich vor Malware?

Die Aktivierung von HTTPS reicht zur Sicherung Ihrer Website nicht aus. Es bedeutet nur, dass ein Angreifer keine Anmeldedaten stehlen kann, indem er jemanden abhört, wenn er sich auf Ihrer Website anmeldet. Cyberkriminelle können weiterhin einen Brute-Force-Angriff innerhalb dieses HTTP-Frames durchführen, um die korrekten Anmeldungen für Ihre Website zu ermitteln.

Die Verwendung von CAPTCHA oder reCAPTCHA vor den Anmeldeformularen auf Ihrer Website ist ebenfalls unzureichend, da diese Dienste leicht automatisiert und umgangen werden können.

Die Begrenzung von Logins oder IPs ist eine weitere Sicherheitsmaßnahme, die Hacker durch Low-and-Slow-Angriffe und verschiedene Automatisierungssysteme leicht umgehen können.

Wenn Sie Datei-Uploads akzeptieren, ist das ein weiteres Problem, um das Sie sich kümmern müssen. Es ist durchaus üblich, dass Angreifer versuchen, in eine Website einzudringen, indem sie entweder einen Virus oder Ransomware-Malware hochladen.



Barracuda

3. Zugriff auf die Infrastruktur

Seit Beginn der COVID-19-Pandemie haben viele Unternehmen VPN für den Zugriff auf intern gehostete Anwendungen eingesetzt. Das kommt vor, wenn es für einige selbst gehostete Anwendungen keinen SaaS-Ersatz gibt. Die Bereitstellung eines VPN-Zugangs von zu Hause aus ist die einzige Möglichkeit, den Geschäftsbetrieb aufrechtzuerhalten. Ohne ordnungsgemäße Identität und Zugriffspraxis ist dieser Ansatz jedoch eine „tickende Zeitbombe, die jederzeit explodieren kann“. Viele bereits gestohlene Zugangsdaten können dafür sorgen, dass Benutzernamen und Passwörter weitergegeben werden, die für den Zugriff auf die Infrastruktur verwendet werden. Dadurch besteht die Gefahr, dass Ihr Netzwerk, Ihre Applikationen und Ihre Daten offengelegt werden können.

4. Laterale Bewegungen

Nachdem sie Ihre Applikation oder Infrastruktur mit gestohlenen Zugangsdaten kompromittiert haben, werden die Hacker versuchen, tiefer in das Netzwerk einzudringen und auf diesem Weg weitere Angriffe durchzuführen. Das ist also der vierte Angriffsvektor, um den Sie sich kümmern müssen. Stellen Sie sich die folgenden Fragen:

- Ist Ihr Unternehmensnetz in ordnungsgemäß geschützte Segmente unterteilt?
- Haben Sie die Multifaktor-Authentifizierung für den Netzwerkzugang aktiviert?

Die richtige Segmentierung Ihres Netzwerks erfordert viel Zeit und Mühe, und es ist leicht, Gründe zu finden, zwei Segmente zu öffnen und den Zugang von einem Segment zum anderen zu ermöglichen. Letztendlich führt dies jedoch dazu, dass der Zugang auf ungewollte Weise geöffnet wird.

Die Multifaktor-Authentifizierung ist eine weitere wichtige Schutzmaßnahme, die Angreifern den Zugang zum Netzwerk verwehrt.

Barracuda

Wie ein Ransomware-Angriff Schwachstellen in Applikationen ausnutzt

Wir behelfen uns eines realistischen, wenn auch erfundenen Ransomware-Angriffs, um zu veranschaulichen, wie ein Angreifer schlechte Anwendungssicherheit ausnutzen könnte, um einen erfolgreichen Ransomware-Angriff zu starten. Wir haben uns für einen gängigen Coupon-Betrug entschieden, d. h. der Angriff macht sich die beliebten Browser-Plug-ins für Coupons im Internet zunutze.

Schritt 1

Der Angreifer erstellt eine Website, die eine legitime Coupon-Website imitiert. Der Angreifer gibt sich als eine beliebte Coupon-Website aus, was mit Domain-Identitätsmissbrauch und automatisiertem Web-Scraping relativ einfach ist. Wir nennen diese gefälschte Website X.

Schritt 2

Der Angreifer sucht nach einer oder mehreren der 10 größten OWASP-Sicherheitslücken, um Zugangsdaten von einer legitimen, aber schlecht geschützten Unternehmenswebsite zu stehlen, die wir Website Y nennen. Schwachstellen wie Fehler in der Authentifizierung und Exposition sensibler Daten ermöglichen es dem Hacker, Zugangsdaten und andere vertrauliche Informationen von der Website Y zu beziehen.

Schritt 3

Der Angreifer verwendet die gestohlenen Zugangsdaten, um einen Credential-Stuffing-Angriff gegen eine legitime E-Commerce-Website, die wir als Website Z bezeichnen, zu starten. Bei diesem Angriff wird versucht, gestohlene Zugangsdaten mit echten Accounts auf diesen Websites abzugleichen.

Schritt 4

Wenn der Angreifer eine Übereinstimmung findet und sich dann in das Konto des Opfers einloggen kann, besteht der nächste Schritt darin, dieses Konto zu nutzen, um Bewertungen beliebter Produkte auf der Website Z zu veröffentlichen. Ein gängiges Beispiel für diesen Schritt ist: „Dieses Produkt ist großartig! Sparen Sie mit diesem Coupon 50 % des Preises, hier klicken.“ Der Link zum Gutschein führt den Besucher auf die Website X, die gefälschte Website aus Schritt eins.

Barracuda

Schritt 5

Die potenziellen Opfer melden sich bei Website Z an, sehen sich die Produktbewertung an und klicken auf den Link zur Website X. Sie können nicht wissen, dass sie auf einer Betrugsseite gelandet sind, außer wenn sie sich den Domainnamen, die URL oder das Seitenzertifikat im Browser genau ansehen. Opfer, die der Seite vertrauen, geben ihre Kontaktinformationen an, um den Coupon zu erhalten. Der Angreifer ist nun im Besitz der E-Mail-Adresse des Betrugsopfers, das eine E-Mail der Website erwartet. Der Angreifer gewinnt das Vertrauen der Person und sie hält weniger nach Betrug Ausschau.

Schritt 6

Das Opfer erhält eine personalisierte E-Mail zum Produkt sowie den versprochenen Coupon. Die Person wird zudem aufgefordert, den E-Mail-Anhang herunterzuladen und zu installieren, um auf den Coupon zugreifen zu können. Bei diesem Anhang kann es sich um eine ausführbare Datei oder eine Browser-Erweiterung handeln, die JavaScript verwendet, um den Angriff auszuführen. Da diese E-Mail vollständig personalisiert und vom Empfänger erwartet wurde, ist sie wahrscheinlich durch traditionelle E-Mail-Abwehrmaßnahmen nicht zu stoppen. Das Betriebssystem des Opfers zeigt zwar den Warnhinweis, keine nicht vertrauenswürdigen ausführbaren Dateien zu installieren, aber zu diesem Zeitpunkt hat das Betrugsopfer wahrscheinlich volles Vertrauen in den Angreifer und klickt sich durch den Installationsprozess.

Schritt 7

Das Opfer installiert den Anhang und der Ransomware-Angriff wird gestartet. Es können mehrere Arten von Angriffen ausgeführt werden, sobald eine ausführbare Datei installiert wurde. Zum Beispiel kann der Master Boot Record (MBR) infiziert oder die Systemtabelle der Datei verschlüsselt werden. Sogar der Versuch, das Betriebssystem zu booten, kann blockiert werden. Kurz darauf wird die Zahlungsaufforderung dem Opfer zugestellt. Der Angreifer wird in der Regel versuchen, diesen Angriff auszuweiten und weitere Zugangsdaten sowie alle anderen Informationen, die im Netzwerk gefunden werden können, zu sammeln. Ist dieser Schritt abgeschlossen, verschlüsselt die Ransomware die Netzwerkdaten.

In diesem Beispiel ist die Ransomware nur deshalb erfolgreich, weil Schwachstellen in der Anwendungssicherheit auf mehreren Websites das überzeugende Szenario überhaupt ermöglichten, vom Web-Scraping einer legitimen Website in Schritt eins und den gestohlenen Zugangsdaten in Schritt zwei über das Credential-Stuffing in Schritt drei, der falschen Produktbewertung und der bösartigen URL in den Schritten vier und fünf bis hin zur Installation der ausführbaren Datei in Schritt sechs und sieben. Die richtige Anwendungssicherheit hätte diesen Angriff an jedem Punkt in der Kette stoppen können.

So sichern Sie Ihre Applikationen und den Zugriff darauf

Ihr Netzwerk sichern

Schützen Sie Ihr Netzwerk vor der Verbreitung von Ransomware durch Netzwerksegmentierung und Intrusion Prevention. Suchen Sie nach einer Firewall-Lösung der nächsten Generation, die:

- eine mehrstufige Schutzfunktion bietet und komplexe Bedrohungen, einschließlich Zero-Day-Angriffe, blockiert,
- Intrusion Prevention und Sandboxing für Malware beinhaltet,
- eine leistungsstarke Netzwerksegmentierung bietet, um laterale Bewegungen innerhalb des Netzwerks zu verhindern.

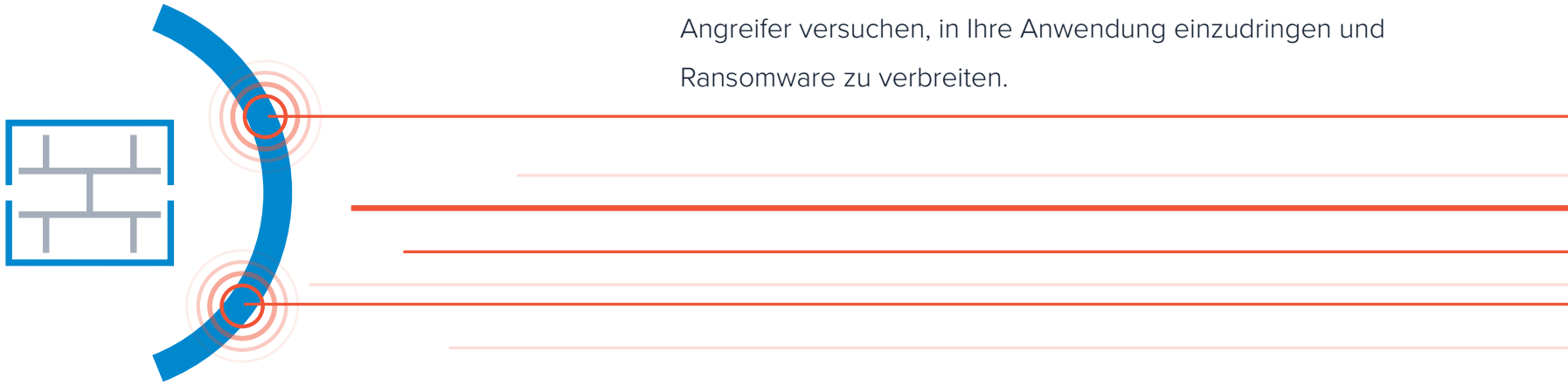
Ihren Anwendungszugriff sichern

Sie sollten Ihren Anwendungszugriff mit einer Zero Trust Network Access (ZTNA)-Lösung absichern, die von jedem Gerät und jedem Standort aus einen sicheren Zugriff auf Anwendungen und Workloads ermöglicht.

Suchen Sie nach einer Lösung, die:

- laufend sicherstellt, dass nur die gewünschte Person mit dem entsprechenden Gerät auf Unternehmensressourcen zugreifen kann,
- rollen- und attributbasierte Zugriffskontrollen nach den Prinzipien der geringstmöglichen Zugriffsrechte erteilt.

ZTNA blockiert unbefugte Zugriffe und verhindert so, dass Angreifer versuchen, in Ihre Anwendung einzudringen und Ransomware zu verbreiten.



Schützen Sie Ihre Web-Applikationen

Zu den besten Möglichkeiten, die Anwendungssicherheit zu gewährleisten, gehört eine Web Application Firewall (WAF), die Ihre Software, Ihre Benutzer und deren Daten schützt, wo auch immer diese sich befinden mögen. Dadurch werden Bot-Angriffe und Denial-of-Service-Attacken unterbunden und Sie erhalten einen weitaus besseren Überblick darüber, was vor sich geht. Wählen Sie eine Lösung mit den folgenden Merkmalen:

Einfach zu implementieren und an Ihre Umgebung anzupassen

Eine WAF kann Sie nicht vollständig schützen, wenn Sie nicht in der Lage sind, sie für Ihre Umgebung zu konfigurieren.

Skalierbar

Unternehmenswachstum, digitale Transformation und andere Faktoren können die Ansprüche an Ihre Anwendungen und Websites erhöhen. Ihre WAF sollte dynamisch mit Ihrem Unternehmen wachsen können.

Umfassender Schutz vor Advanced Threats

OWASP-Top-Ten-Schutz und DDoS-Schutz auf Anwendungsebene sind die Grundvoraussetzungen, die man von einer guten WAF erwarten sollte. Für einen umfassenden Schutz sollten Sie jedoch nach einer Lösung suchen, die auch Zero-Day-Angriffe, Credential Stuffing, Datenlecks, bösartige Bots und mehr abwehrt.

Einfach zu aktualisieren

Eine WAF sollte über regelmäßige Firmware-Updates verfügen, um die Sicherheit und die Fähigkeiten des Geräts zu verbessern. Ideal ist eine gehostete Lösung, die automatisch ohne Eingriff des Administrators aktualisiert wird.

Kontinuierliche Bedrohungsanalyse

Jeden Tag werden neue Angriffsarten erdacht, die sich innerhalb weniger Stunden weltweit verbreiten können. Ihre WAF sollte Echtzeit-Updates zu diesen Angriffen erhalten und maschinelles Lernen einsetzen, um sich an Varianten anzupassen.

Eine gute Web Application Firewall blockiert gängige Schwachstellen in Web-Applikationen und Zero-Day-Bedrohungen und verhindert dadurch, dass sich Ransomware in Ihren Systemen ausbreitet.

3. Schritt: Sichern Sie Ihre Daten

Am Anfang jeder ernsthaften Strategie zum Schutz vor Ransomware sollten Überlegungen zu Backup und Disaster Recovery stehen. Leider wissen das auch Kriminelle.

Während der Phase, in der die Angreifer ihren Opfern „auflauern“ und sich einen Überblick über ihr Netzwerk verschaffen, liegt ihr Fokus auf den Backup-Lösungen. Besonders wichtig für die Angreifer ist hierbei die Backup-Verwaltungskonsole, über die sie Zugriff auf die Backup-Pläne, -Konfiguration und -Aufbewahrungsrichtlinien erhalten und in der sie die Möglichkeit haben, mit dem Löschen von Daten zu beginnen.

Barracuda

Angreifer haben es zudem auf den Backup-Speicher selbst abgesehen, da sie darauf hoffen, Ihren primären Backup-Server und alle sekundären Disaster-Recovery-Backup-Kopien, die Sie aufbewahren, zu löschen. Sobald sie in den Besitz der Active-Directory-Passwörter gelangen und Benutzer sich infolgedessen nicht mehr in ihren Konten anmelden können, haben die Angreifer ihr Ziel erreicht: sie haben die Kontrolle erlangt.

Außerdem ist der Irrglaube, dass Ihre Daten in der Cloud sicher vor Ransomware-Angriffen sind, immer noch weit verbreitet. Das stimmt jedoch nicht.

Ein Kind kann beispielsweise beim Surfen im Internet über das Schul-Tablet oder den Schul-Laptop zu Hause ganz einfach dazu verleitet werden, aus Versehen auf einen schädlichen Link zu klicken. Wenn das Gerät mit OneDrive als Teil des Office 365-Kontos der Schule verbunden und synchronisiert ist, kann eine Ransomware-Datei automatisch in OneDrive hochgeladen werden und die in der Microsoft Cloud gespeicherten Dateien und Daten der Schule verschlüsseln.

Betrachten Sie die Notfallwiederherstellung als einen wichtigen, strategischen Teil Ihrer Infrastruktur. Testen Sie sie regelmäßig und unter realistischen Bedingungen. Nehmen Sie also eine tatsächliche Wiederherstellung vor, und prüfen Sie nicht nur, ob sie funktioniert.

Barracuda

Wir haben auch andere Beispiele gesehen, bei denen SharePoint, Exchange und andere Datenquellen betroffen waren. Wenn Netzlaufwerke dann auch noch über die Funktion „Mit Explorer öffnen“ den Dokumentbibliotheken in Office 365 zugeordnet sind, kann die Ransomware auch nach Dateien auf verbundenen Laufwerken suchen und diese infizieren.

Auch Daten aus der Cloud und SaaS-Daten können durch Ransomware verschlüsselt werden. Microsoft garantiert die Verfügbarkeit des Dienstes, empfiehlt Ihnen jedoch, Ihre Daten mit einer Backup-Lösung eines Drittanbieters zu sichern. Sie können Ihre Daten in Microsoft Office 365 speichern, aber Office 365 ist nicht dafür ausgelegt, ganze Instanzen wiederherzustellen, was nach einem Ransomware-Angriff erforderlich sein kann.

Sie müssen also die Backup-Daten angemessen schützen und isoliert aufbewahren. Bedenken Sie, wie oft Systeme gespiegelt werden müssen und wie schnell Sie Systeme aus diesen Sicherungen wiederherstellen können.

Sie müssen sicherstellen, dass die Wiederherstellung von Systemen aus Sicherungsversionen innerhalb eines angemessenen Zeitrahmens und anhand ausreichend aktuelle Informationen tatsächlich möglich ist. Sie müssen also die Kontrolle übernehmen und die Dinge in die Hand nehmen. Es genügt nicht, die Protokolle zu überprüfen, um festzustellen, ob die Daten oft genug und genau genug repliziert werden.

Führen Sie realistische Prüfungen durch, um zu beweisen, dass die Systeme funktionieren. Möglicherweise entscheiden Sie sich für eine Abteilung oder sogar nur für eine Anwendung, anstatt sämtliche Systeme stillzulegen. Entscheidend ist jedoch, dass Sie sich darauf verlassen können, dass die Systeme rechtzeitig wiederhergestellt werden können.

Dies ist Ihr Schutzwall. Selbst wenn alles andere zusammenbricht, können Kriminelle Sie nicht ausbremsen, wenn Sie eine aktuelle und sichere Datensicherung haben.

Betrachten Sie die Notfallwiederherstellung als einen wichtigen, strategischen Teil Ihrer Infrastruktur. Testen Sie sie regelmäßig und unter realistischen Bedingungen. Nehmen Sie also eine tatsächliche Wiederherstellung vor, und prüfen Sie nicht nur, ob sie funktioniert.

Was benötigen Sie in einer Backup-Lösung?

Um die im Zusammenhang mit Ransomware auftretenden Risiken zu minimieren, benötigen Sie eine umfassende Backup-Lösung, die Folgendes beinhaltet:

Unveränderbarer Speicher

Selbst wenn ein Angreifer Zugriff auf Ihre Backups erlangt, kann er die Daten nicht verändern oder löschen.

„Air-Gapped“ Cloud

Bewahren Sie eine Kopie Ihres Backups in einer sicheren Cloud auf, welche sich wiederum in einem isolierten Netzwerk befindet.

Multi Factor Authentication (MFA)

Sichern Sie die Accounts und Zugangsdaten, die für den Zugriff auf das Backup benötigt werden.

Redundanz

Replizieren Sie Ihre on-premises und in der Cloud gespeicherten Backups zusätzlich an einem anderen Speicherort.

Rollenbasierte Zugriffskontrolle

Wenden Sie auf alle Benutzer, die Zugriff auf das Backup-System haben, das Prinzip der geringstmöglichen Zugriffsrechte an.

Barracuda

Fazit

Auch wenn Ihr Unternehmen über eine Cyber-Versicherung oder andere Ressourcen für die Zahlung von Lösegeld verfügt, ist die Annahme, dass durch die Zahlung eines Lösegelds Ihre Daten tatsächlich wiederhergestellt werden, hochriskant. Es gibt keine Garantie dafür, dass Hacker Ihre Daten wirklich entschlüsseln, sobald das Lösegeld bei ihnen eingetroffen ist. Selbst in den Fällen, in denen Angreifer ihr Versprechen eingehalten haben, zeigen jüngste Untersuchungen, dass 80 % der Unternehmen, die Lösegeld gezahlt haben, erneut angegriffen wurden.

Selbst wenn Sie alle oben genannten Maßnahmen ergriffen haben, werden Sie immer noch angegriffen werden. Selbst wenn Sie den besten Schutz haben, ist es angebracht, sich auf das Schlimmste vorzubereiten. Kriminelle verfügen über Millionenbeträge, die sie investieren können, um in Ihre Systeme einzudringen. Man kann sich nur vernünftig vorbereiten, wenn man davon ausgeht, dass man eines Tages erfolgreich angegriffen wird.

- [ ] Wer ist Teil Ihres Teams für Ransomware-Response?
- [ ] Wer wird angerufen, wenn etwas an einem Wochenende oder Feiertag passiert?
- [ ] Wer ist zuständig?
- [ ] Wann informieren Sie Kunden und Lieferanten?
- [ ] Wer berät Sie in Rechtsfragen?
- [ ] Müssen Sie eine Aufsichtsbehörde oder die Polizei benachrichtigen?
- [ ] Muss von Anfang an ein PR-Mitarbeiter involviert werden?

Sie müssen sich Gedanken darüber machen, was an diesem Tag passiert. Sie benötigen einen Plan, um das Lösegeld nicht bezahlen zu müssen.

Ähnlich wie bei einer Brandschutzübung ist der richtige Zeitpunkt zum Üben nicht der, zu dem das Büro in Flammen steht. Allerdings ändern sich die derzeitigen und die wahrscheinlichen Angriffe im Laufe der Zeit, weshalb Ihre Strategie und Ihre Verteidigungstaktiken regelmäßig aktualisiert werden müssen. Laden Sie sich unsere Ransomware-Checkliste herunter, um Ihren Plan in Angriff zu nehmen.

Barracuda

Seien Sie darauf vorbereitet, auf einen Angriff zu reagieren

Sie müssen sich Gedanken darüber machen, was passiert, sobald ein Angriff erkannt wird, und was passiert, wenn dieser Angriff zu einem Sicherheitsverstoß wird. Lässt sich die Gefahr eindämmen oder auf einen Teil Ihrer Infrastruktur beschränken, indem der Netzwerkverkehr gestoppt wird? Müssen Sie Systeme vorübergehend vom Netz nehmen? Wenn ja, wer übernimmt die Verantwortung dafür?

Eine schnelle Reaktion ist hier absolut entscheidend. Ein gezieltes, schnelles Vorgehen. Sie sollten nicht auf einen Rückruf Ihres CTO warten müssen. Jeder muss wissen, was in dem Moment zu tun ist.

Wenn dies schnell genug erfolgt, können Sie die Verschlüsselung vielleicht sogar verhindern. Außerdem benötigen Sie einen Plan zur schnellen Überprüfung Ihrer Systeme, um sich einen genauen Überblick darüber zu verschaffen, was vor sich geht.

Moderne Angreifer neigen dazu, mehr als eine Angriffsart gleichzeitig einzusetzen. Es kann sein, dass Sie gerade mit einem Denial-of-Service-Angriff beschäftigt sind, und gleichzeitig ein Ransomware-Angriff auf ein anderes Ziel gerichtet ist. Wenn Sie wissen, was wo passiert ist, können Sie darüber nachdenken, was Sie tun müssen, um die Malware zu beseitigen und die Systeme wieder in Betrieb zu nehmen.

Nach der Wiederherstellung von Systemen und Daten, sei es aus einer Sicherungskopie oder durch eine frühzeitige Abgrenzung des Angriffs, und der Überprüfung auf beschädigte oder fehlende Daten, ist es an der Zeit, mit der Forensik zu beginnen.

Beurteilen Sie, wie wirkungsvoll Ihre Abwehrmaßnahmen gegen einen realen Angriff waren. Analysieren Sie, was gut funktioniert hat, was nur durch Zufall geklappt hat und was sich als ungeeignet erwiesen hat. Überlegen Sie, wie Sie beim nächsten Mal besser und schneller reagieren können.

Wenn Sie die richtigen Systeme einsetzen, werden Sie eine Fülle von forensischen Daten haben, die Sie auswerten können. Vielleicht haben Sie sogar genug Informationen, damit die Polizei Ermittlungen aufnehmen kann. Unabhängig davon, über welche Daten Sie verfügen, sollten Sie sich die Zeit nehmen, eine Nachbesprechung mit dem Notfallteam durchzuführen und die daraus gezogenen Erkenntnisse zu reflektieren.

Es geht hier wie gesagt nicht nur um Technologien, sondern auch um Menschen und Prozesse. Müssen Sie sich noch einmal Gedanken über das Konzept Ihrer Mitarbeiterschulungen machen? Hat Ihr Notfallteam einwandfrei funktioniert, oder muss es verstärkt werden?

Bleiben Sie auf dem Laufenden

Moderne Verteidigungsstrategien müssen aktiv sein, nicht nur reaktiv. Sie benötigen größtmögliche Transparenz in Bezug auf Ihre Sicherheitssysteme. Sie müssen überwachen, was wann und wie oft passiert. Sie müssen Ihre Mitbewerber im Auge behalten, denn Ransomware-Angreifer haben es oft auf einen bestimmten vertikalen Markt oder eine bestimmte Region abgesehen. Außerdem sollten Sie sich mit Hilfe von Ressourcen wie dem Barracuda-Blog über die neuesten Bedrohungen, Trends und Branchennachrichten auf dem Laufenden halten.

Daten sind für eine erfolgreiche Sicherheitsstrategie von entscheidender Bedeutung. Wahrscheinlich wird sich die Haltung oder das Profil Ihres Unternehmens im Laufe der Zeit ändern. Sie müssen darauf vorbereitet und entsprechend informiert sein, um bei Bedarf Änderungen vornehmen zu können. Security-as-a-Service kann Ihnen einen Teil der mühsamen Aufgaben abnehmen, die damit verbunden sind, mit den Entwicklungen Schritt zu halten. Insbesondere, da sich die heutige Cybersicherheitslandschaft schneller verändert als je zuvor.

Für bestimmte Unternehmen, die sehr aktiv sind oder ein hohes Risikoprofil aufweisen, könnte dies bedeuten, dass sie Vollzeitmitarbeiter dafür einsetzen müssen, sich mit dem Thema Threat Intelligence zu beschäftigen, um frühzeitig vor möglichen Angriffen zu warnen.

Für die meisten Unternehmen geht dies jedoch über das erforderliche Maß hinaus. Entscheiden Sie sich für einen geeigneten Partner und sorgen Sie dafür, dass die Grundlagen vorhanden sind. Im Gegensatz zu dem, was wir in Film und Fernsehen zu sehen bekommen, sind echte Angreifer keine bösen Superhirne, die mit Vorliebe die ausgefeiltesten Sicherheitssysteme aushebeln. In den meisten Fällen hoffen sie auf eine leichte Beute durch jemanden, der nicht aufpasst oder nicht in die richtigen Sicherheitsmaßnahmen investiert hat.

Wenn Sie diese drei Schritte befolgen (Schutz Ihrer Zugangsdaten, Sicherung Ihrer Web-Applikationen und den Zugriff darauf, Sicherung Ihrer Daten), ist nicht garantiert, dass Sie nicht Opfer von Ransomware werden. Aber Sie müssen garantiert kein Lösegeld zahlen, um Ihre Daten wiederzubekommen.

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir glauben, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu kaufen, zu implementieren und zu verwenden sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit unseren Kunden wachsen und sich anpassen.

Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Somit können Sie sich darauf konzentrieren, ihr Geschäft auf die nächste Stufe zu bringen. Weitere Informationen finden Sie unter de.barracuda.com.

Barracuda
Your journey, secured.