WatchGuard™

PERFEKTIONIEREN SIE IHRE VERTEIDIGUNGSSTRATEGIE

EIN KLEINER LEITFADEN FÜR MEHR IT-SICHERHEIT – FÜR SIE UND IHRE ANWENDER

b.o.c.
IT-SECURITY

Übung macht den Meister

Verteidigungskenntnisse und -übungen

Wenn Sie eine effiziente Verteidigung wünschen, müssen Sie Ihre Mitarbeiter und Belegschaft auf alle Arten von Angriffen vorbereiten. Es folgen einige wichtige Sicherheitselemente, die Sie bei der Planung Ihrer Sicherheitsschulung berücksichtigen sollten:

1 Kennwortsicherheit

2 Phishing-Angriffe

3 Erweiterte Malware

4 WLAN-Sicherheit

5 Desktop-Sicherheit

1. https://www.rapid7.com/fundamentals/security-awareness-training/

Zentrale Verteidigungskenntnisse[2]

StaySafeOnline.org enthält einige wichtige Angaben, an die Sie Ihre Mitarbeiter erinnern sollten, damit sie sich vor Angriffen schützen können:

1 Halten Sie Ihren Computer aufgeräumt

Als IT-Team sollten Sie sicherstellen, dass eingeschränkt wird, was einzelne Benutzer auf ihren Geräten installieren können. Diese Arten von Beschränkungen werden oft über Berechtigungen festgelegt, die der IT-Administrator voreinstellt.

2 Befolgen Sie gute Kennwortpraktiken

Verwenden Sie Passphrasen, Kapitalisierung, Symbole, Ziffern, sogar Listen zufälliger Wörter – achten Sie darauf, dass die Kennwörter für Ihre dienstlichen und privaten Konten unterschiedlich sind!

Tipp:

Verwenden Sie eine Passphrase mit einer Kombination aus Ziffern, Groß- und Kleinbuchstaben und ggfs. Sonderzeichen anstelle eines einfachen Wortes. Diese sind oft schwerer zu entschlüsseln!

3 Erwägen Sie die Multifaktor-Authentifizierung

Kennwörter haben beim Schutz Ihrer Organisation nur eine beschränkte Rolle. Lösungen, wie die Multifaktor-Authentifizierung, können zusätzliche Verteidigungslinien gegen unerwünschten Zugriff aufbauen.

4 Im Zweifelsfall nicht öffnen!

Seien Sie sehr vorsichtig, wenn Sie Links in E-Mails, Tweets, Posts, Online-Werbung oder Nachrichten öffnen. Sie sollten auch skeptisch sein, wenn Sie einen Anhang von einem Absender öffnen, den Sie nicht kennen.

Tipp:

Kopieren Sie den Hyperlink in einen neuen Browser, anstelle auf einen Link zu klicken. Dadurch ist einfacher zu sehen, ob der Link tatsächlich zum angegebenen Ziel führt.

5 Sperren Sie den PC, wenn Sie fortgehen

Achten Sie stets darauf, dass Ihr Computer gesperrt ist, wenn Sie Ihren Schreibtisch verlassen, damit keine unberechtigten Personen Zugriff erhalten.

6 Sichern Sie Ihre Arbeit

Zwar sollten Sie automatische Backups eingerichtet haben, aber es schadet nie, Ihre Mitarbeiter auch dazu anzuregen, selbst regelmäßige Backups durchzuführen!

7 Melden Sie sich!

Melden Sie der IT-Abteilung seltsame Aktivitäten oder Verhaltensweisen auf Ihrem Gerät sobald wie möglich! Je schneller das Team darüber informiert wird, desto besser die Chance, dass Schäden eingegrenzt werden können.

2 https://staysafeonline.org/business-safe-online/train-your-employees

Übungen zur Verteidigung gegen Phishing-Angriffe[3]

Wie bereits besprochen, sind Phishing-Angriffe eine der häufigsten Methoden, die heute von Hackern eingesetzt werden. 2016 begannen tatsächlich 91 % aller Cyberattacken mit einer Phishing-E-Mail. Hier finden Sie einige Tipps für Ihre Mitarbeiter, mit denen diese bösartigen E-Mails erkannt werden können.[4]

1

Welches Gefühl vermittelt die E-Mail?

Hacker nutzen oft die Emotionen des Empfängers, um ihn zur Beachtung der E-Mail zu verleiten. Ob sie Neugier, Furcht, Dringlichkeit oder sogar Gier erwecken, E-Mails mit so einem Ton verstecken oft bösartige Absichten.

2

Prüfen Sie die Standardelemente der E-Mail auf Diskrepanzen

Prüfen Sie die Domäne des Senders und die E-Mail-Signatur auf seltsame oder ungewöhnliche Informationen.

3

Enthält sie Grammatikfehler?

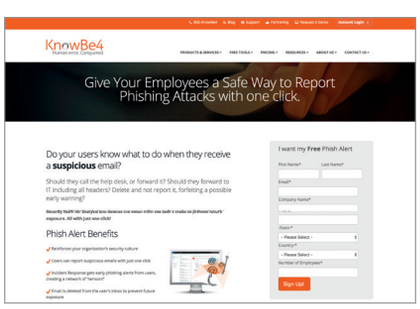
Zahlreiche Grammatikfehler sollten ein Warnzeichen sein, dass dies eine Phishing-E-Mail sein könnte, besonders wenn dies mit den beiden anderen Tipps oben auftritt.

Die Profis einbringen

Mitarbeiterschulung ist ein erster wichtiger Schritt, Ihre Organisation zur Verteidigung gegen erweiterte Angriffe aufzustellen. Sie können mit zahlreichen Unternehmen zusammenarbeiten, um Kundenprogramme zu schaffen, die speziell auf Ihre Organisation zugeschnitten sind.

Es soll nicht zu teuer werden? Unternehmen wie KnowBe4[5] und PhishMe[6] bieten verschiedene kostenlose Ressourcen, die Ihnen bei der Weiterbildung und Schulung Ihrer Mitarbeiter helfen, wie:

- » Poster zur Bewusstseinsbildung
- » Kostenlose Phishing-Tests
- » Tests auf schwache Kennwörter
- » Ransomware-Simulator
- » Gratis-Schulungsmodule



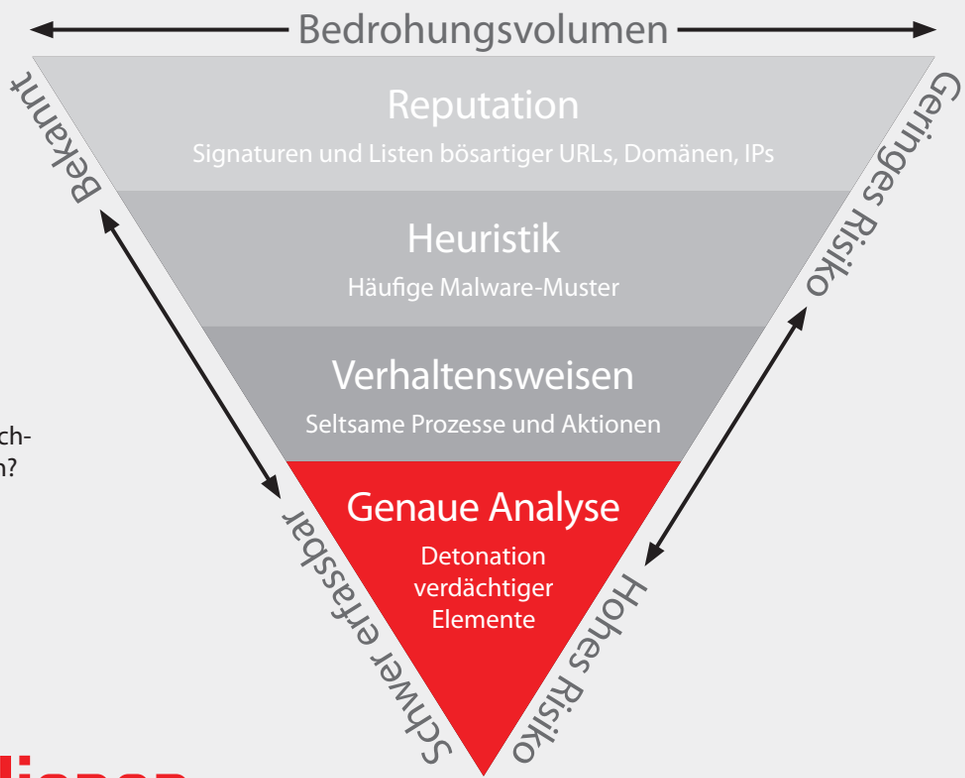
KnowBe4 bietet auch einen kostenlosen Phishing-Alarmknopf, mit dem Mitarbeiter verdächtige E-Mails sicher und einfach an die IT- oder Sicherheitsteams weiterleiten können.

3 https://phishme.com/wp-content/uploads/2016/10/PM-How-to-spot-a-phish-Infographic.zip
4 https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704?
5 https://www.knowbe4.com
6 https://phishme.com/

Vorbereiten Ihrer Verteidigungslinien

Reputation

Die Abwehr bekannter Bedrohungen ist zwar relativ einfach, aber auch sehr wichtig. Hacker wissen, dass Organisationen und Einzelpersonen oft beim Nachbessern ihrer Systeme nachlässig sind und sich gegenüber diesen Angriffen verletzlich machen. Nach Angabe von AV-Test gibt es derzeit mehr als 700 Millionen bekannte Malware-Varianten.[7] Haben Sie Ihre Verteidigungslinien eingerichtet, um gegen alle geschützt zu sein?



Es gibt mehr als

700 Millionen

bekannte Malware-Varianten

Es müssen Lösungen implementiert werden, um das Netzwerk und die Endpunkte vor dieser Art von Angriffen zu schützen, einschließlich Signatur-Abwehren sowie Listen bösartiger URLs, Domänen und IP-Adressen. Diese Abwehrmaßnahmen gibt es in zahlreichen verschiedenen Formen, Größen und zu unterschiedlichen Preisen. Hier sind einige „Unverzichtbare“:

1 Endpunkt-Antivirus

Dies ist wahrscheinlich die am weitesten verbreitete Signaturverteidigung für den Endpunkt. Diese Listen von Signaturen können genutzt werden, um Angriffe vor dem Benutzereingriff zu stoppen. Die meisten dieser Lösungen werden regelmäßig aktualisiert, um sicherzustellen, dass sie die neuesten Patches enthalten.

2 Intrusion Prevention Service (IPS)

Prüfung des Netzwerkverkehrs auf unterster Ebene, um bekannte Bedrohungen zu identifizieren, indem Verkehrsmuster mit Signatur-Datenbanken verglichen werden.

3 Web-Reputation

Prüft die Ziele von ausgehenden Verbindungen und identifiziert deren Bedrohungsstufe basierend auf Intelligence Feeds. Verkehr zu URLs mit schlechtem Ansehen wird sofort blockiert.

4 URL-Filterung

Abfrage von URL-Kategorien und Unterkategorien, um Zugriff auf die URL basierend auf Richtlinieneinstellungen wie Benutzer, Gruppe und Plan zu gestatten oder zu blockieren.

7 https://www.av-test.org/en/statistics/malware/

Heuristik und Verhaltensweisen

Von Hackern werden laufend neue Malware-Varianten geschaffen. AV-Test berichtet, dass jeden Tag mehr als 390.000 neue Malware-Varianten registriert werden. Eine Verteidigung dagegen scheint hoffnungslos zu sein. Es gibt jedoch auch einige Lösungen, die Ihnen beim Kampf gegen Bedrohungen, für die noch keine Signatur erstellt worden ist, zur Seite stehen.

Obwohl die Malware-Varianten sich alle auf gewisse Weise unterscheiden, folgt die Bedrohung selbst einem üblichen und damit erkennbaren Muster von Ereignisabläufen während des Angriffs. Heuristische und Verhaltenserkennungsmethoden analysieren die Malware, um diese Prozesse und Aktionen zu erkennen und zu ermitteln, ob die Malware bösartig ist. Bedrohungen, die aktiv Registrierungsschlüssel erstellen, die Host-Datei verändern, einen Prozess erstellen oder sogar Code entpacken, werden als bösartig angesehen und beseitigt.

Hier finden Sie einige Erkennungsmethoden, die Heuristik und/oder Verhaltensweisen nutzen:

1

Gateway AV

Nutzt sowohl signaturbasiertes als auch heuristisches Scannen von Dateien, um bekannte Malware und Riskware zu identifizieren. Nachdem eine übereinstimmende Signatur erkannt wurde, wird die Verbindung blockiert oder die Datei entsorgt.

2

Spam Prevention

Erkennt übliche bösartige Muster in Mail-Kopfzeilen, die auf Spam hinweisen.

3

Endpunkt-Heuristik und Verhaltenserkennung

Überwacht Endpunkte auf Dateien mit bösartigem Code und Anzeichen von Verhaltensweisen, die in Malware häufig zu beobachten sind.

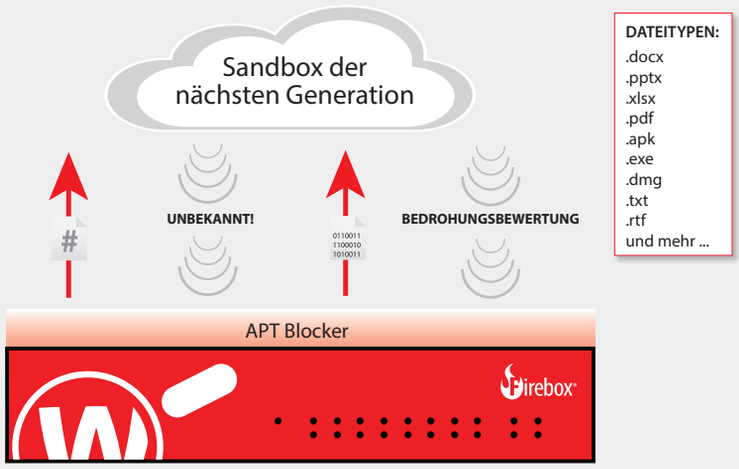
Gründliche Analyse

Schwer erfassbare, raffinierte Bedrohungen benötigen professionelle Erkennungsmethoden. Diese Bedrohungen sind oft speziell zur Vermeidung herkömmlicher Erkennungsmethoden anhand von Signaturen, Heuristik und Verhaltensweisen ausgelegt. Wie können Sie sich gegen solche Angriffe zur Wehr setzen?

Methoden zur gründlichen Analyse können verdächtige Elemente, die in Ihrem Netzwerk und an einem Endpunkt gefunden werden, in einer Cloud-Sandboxing-Umgebung sicher detonieren. Nachdem die Datei detoniert wurde, kann bestimmt werden, ob das Ereignis harmlos oder bösartig war, und die Datei kann ggfs. beseitigt werden.

Netzwerk-Sandboxing

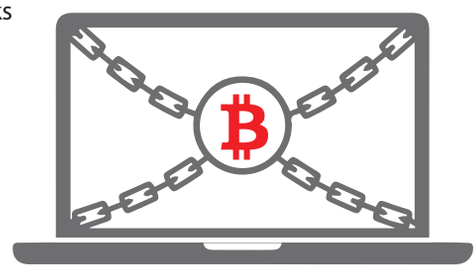
Verhaltensanalysen bestimmen, ob eine Datei bösartig ist, identifizieren und senden verdächtige Dateien in eine cloudbasierte Sandbox, in der der Code emuliert, ausgeführt und analysiert wird, um sein Gefahrenpotenzial zu ermitteln. Wenn festgestellt wird, dass die verdächtige Datei bösartig ist, wird die Bedrohung schnell beseitigt, bevor Schäden entstehen.



Spielzüge zur Abwehr von Angriffen

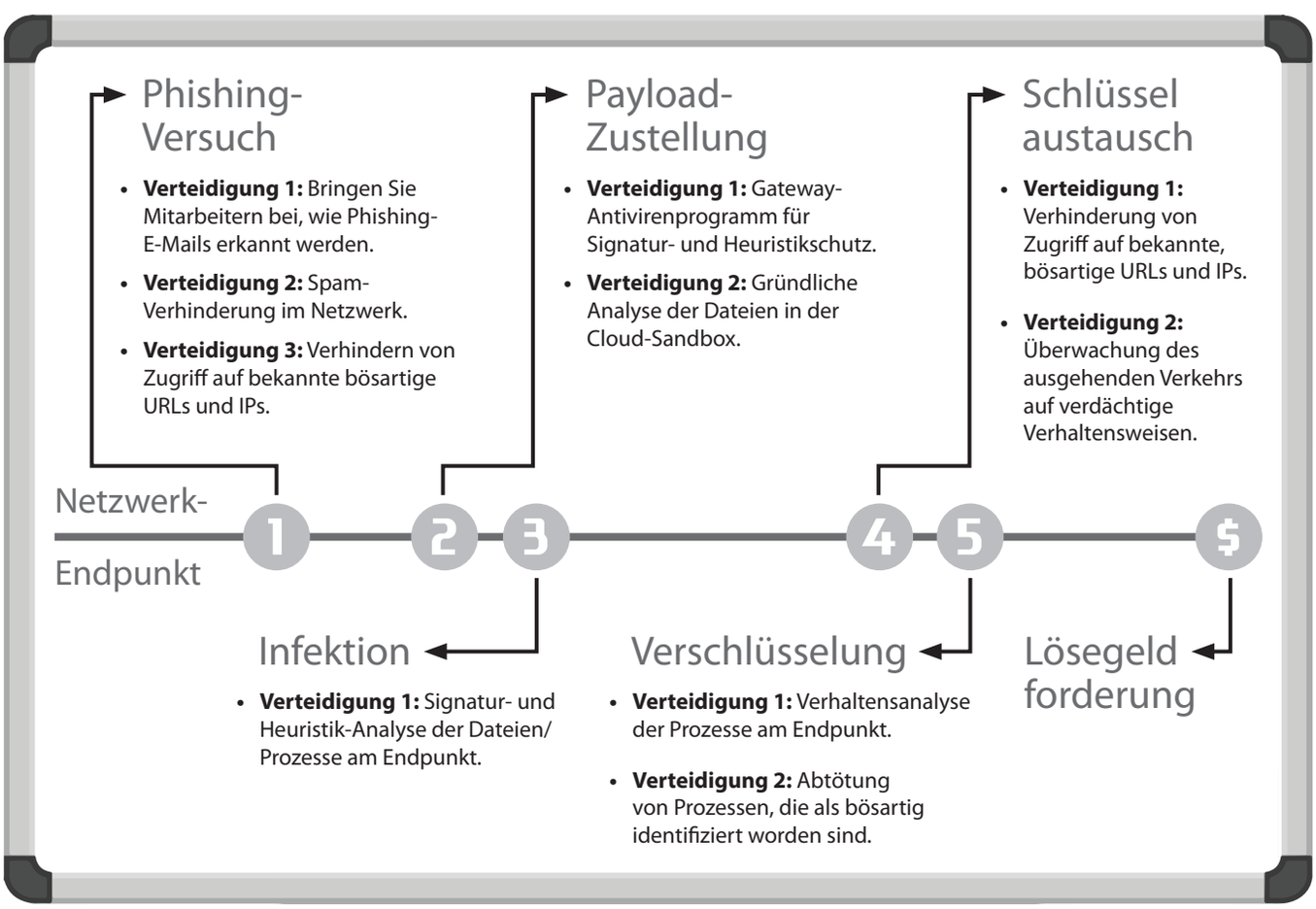
Spielzug 1: Abwehr von Ransomware

Ransomware ist eine besonders perfide Form des modernen Malware-Angriffs, bei der ein Gerät in Geiselhaft genommen wird, indem entweder der Benutzer ganz ausgesperrt wird oder die Dateien verschlüsselt werden, damit sie nicht verwendet werden können. Neueste Crypto-Ransomware-Stämme folgen einem typischen Infizierungspfad durch den Benutzer Opfer einer Phishing-Kampagne werden: Wenn er entweder auf einen Link klickt oder eine Datei in einer bösartigen E-Mail herunterlädt. Damit beginnt ein Prozess, bei dem die Malware über einen Dropper an den Endpunkt geliefert wird und dann versucht, mit einem Befehls- und Steuerserver außerhalb des Zielnetzwerks zu kommunizieren. Wenn dies erfolgreich ist, liefert der Befehls- und Steuerserver einen Verschlüsselungscode, die Dateiverschlüsselung beginnt und das Opfer erhält eine Lösegeldforderung für die Rückgabe der Daten.



Wie aus Abbildung 1 ersichtlich ist, sind Ransomware-Attacken komplizierte, mehrstufige Vorgänge. Jede der fünf Phasen einer Attacke bieten eine Gelegenheit, die Attacke zu erkennen und deren Erfolg möglicherweise zu verhindern, wenn geeignete Sicherheit und Richtlinien vorhanden sind.

Abbildung 1:



Spielzug 2: Schutz von empfindlichen Daten und Systemen

Einer der bedeutendsten und öffentlichkeitswirksamsten Angriffe im letzten Jahrzehnt war der Angriff auf die Handelskette Target im Jahre 2013. Hacker drangen in das Netzwerk von Target ein, installierten Malware direkt in die Registrierkassensysteme und stahlen 40 Millionen Kreditkartennummern, bevor der Angriff entdeckt wurde.

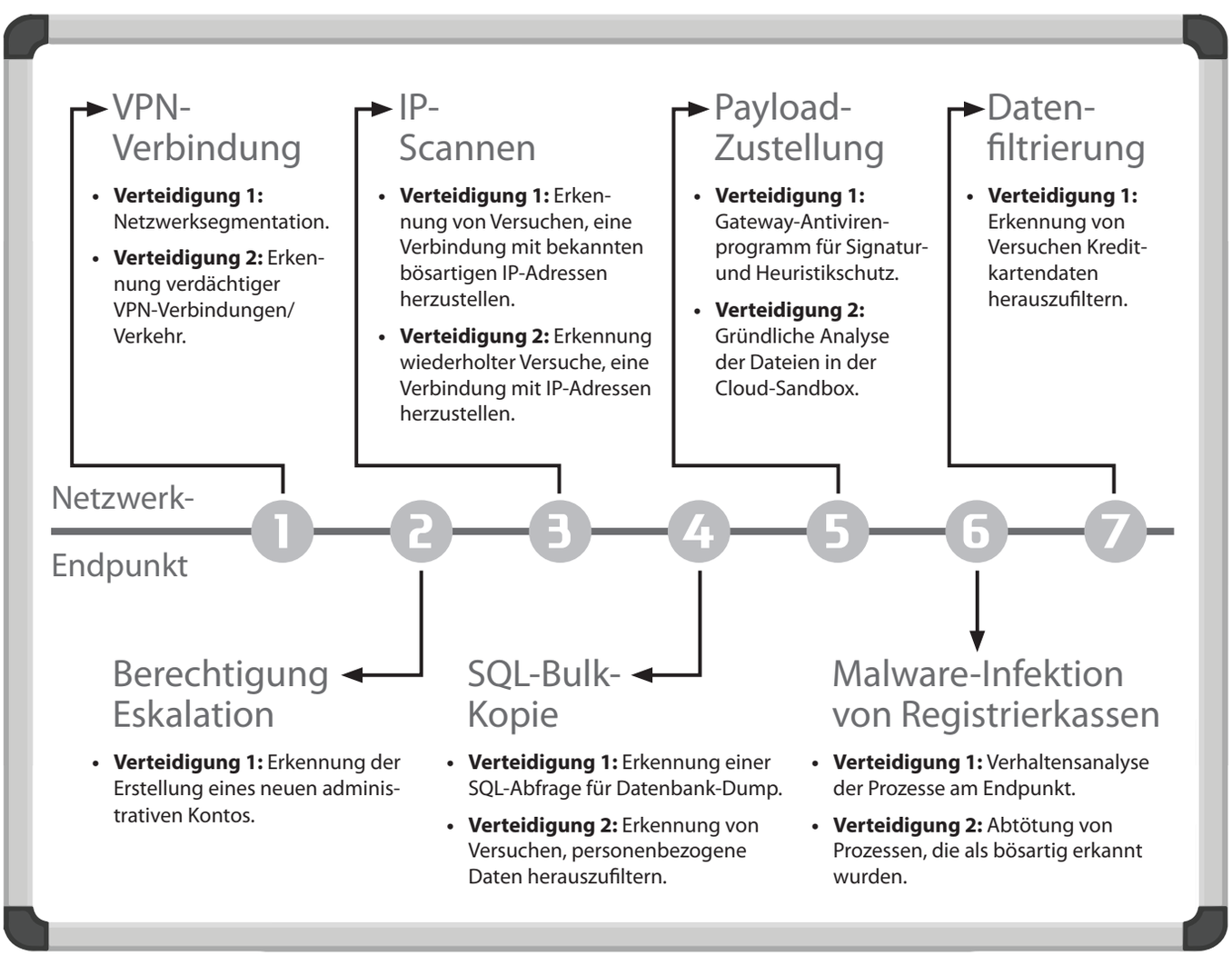
Der Angriff begann, als VPN-Anmeldeinformationen von einem unabhängigen Lieferanten gestohlen wurden. Mit diesen Anmeldeinformationen konnten die Angreifer in das Konzernnetzwerk von Target eindringen und sich anderen empfindlichen ausnutzbaren Stellen zuwenden. Zuerst wurde eine Datenbank mit mehr als 70 Millionen Kundendatensätzen kopiert, einschließlich Namen, Adressen, E-Mail-Adressen und Telefonnummern. Danach implementierten die Angreifer Malware, um in die Registrierkassen einzudringen und Kreditkarteninformationen zu erfassen.

70 Millionen

Kundendatensätze, einschließlich Namen, Adressen, E-Mail-Adressen und Telefonnummern wurden 2013 beim Angriff auf Target kopiert.

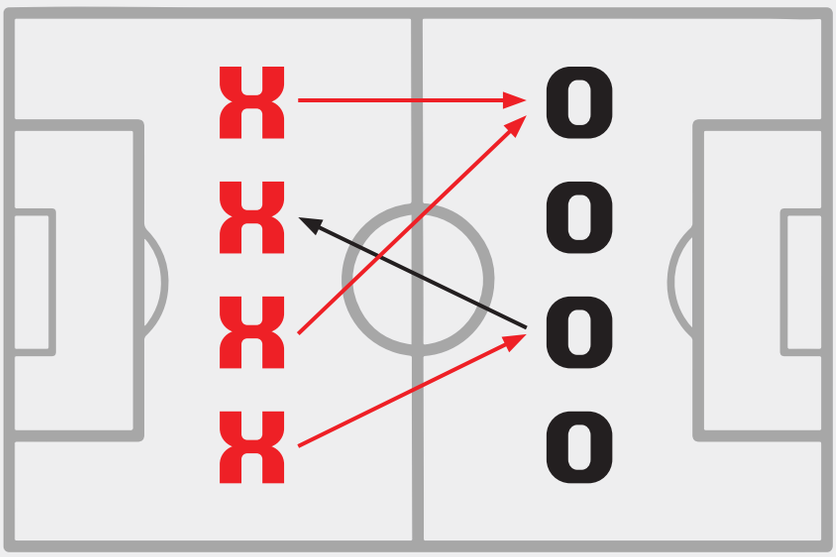
Abbildung 2 zeigt die verschiedenen Stellen des Netzwerks und der Endpunkte, an denen bei einem Angriff ähnlich wie bei Target 2013 die Erkennung und damit die Abwehr stattfinden könnte.

Abbildung 2:



Sind Sie bereit anzufangen?

Wir haben gerade VIELE Informationen durchgearbeitet, wie Sie Ihre Organisation vor raffinierten Malware-Angriffen schützen können. Um all das ein wenig einfacher zu machen, finden Sie hier eine Prüfliste, die Ihnen bei der Beurteilung Ihrer derzeitigen Verteidungsstrategie helfen kann. Wir raten Ihnen, Ihre Strategie alle sechs Monate neu zu überdenken. Daher haben wir Platz für Prüfungen nach 6 und 12 Monaten gelassen.



Strategie-Check: Heute und in 6/12 Monaten

JETZT NACH 6 MONATEN NACH 12 MONATEN

☐ ☐ ☐ Backups

- Abschließen der Weiterbildung
- Sicherstellung, dass automatische Backups eingeplant sind

☐ ☐ ☐ Kennwörter

- Weiterbildung der Mitarbeiter über die Wichtigkeit starker Kennwörter
- Festlegung einer Standard-Richtlinie für die Kennwortlänge und -aktualisierung
- Implementierung von Multifaktor-Authentifizierung zur Gewährleistung von Sicherheit auch bei schwachen Kennwörtern

☐ ☐ ☐ Weiterbildung zu Phishing-E-Mail

- Weiterbildung der Mitarbeiter: Wie sehen Phishing-E-Mails aus?
- Testen der Mitarbeiter anhand harmloser Phishing-E-Mails

☐ ☐ ☐ WLAN

- Bewertung der WLAN-Sicherheitslösung
- Weiterbildung der Mitarbeiter über die Risiken von öffentlichem WLAN

JETZT NACH 6 MONATEN NACH 12 MONATEN

☐ ☐ ☐ Verteidigung gegen bekannte Bedrohungen

- Sicherstellung, dass Signatur-Lösungen wie Virenschutzprogramme und Intrusion Prevention Systeme aktuell sind
- Prüfung, welche Websites in den URL-Filtertools blockiert oder gestattet sind

☐ ☐ ☐ Verteidigung gegen unbekannte Bedrohungen

- Sicherstellung, dass eine Anti-Spam-Lösung implementiert ist
- Bewertung, welche Tools verwendet werden, die eine heuristische Analyse und eine Erkennung der Verhaltensweisen umfassen

☐ ☐ ☐ Verteidigung gegen schwer erfassbare Bedrohungen

- Bewertung der Netzwerk-Sandboxing-Lösung
- Prüfung der Abhilfeverfahren und -Richtlinien

WatchGuard Security Services

WatchGuard bietet verschiedene Sicherheitsdienste, damit Ihr Sicherheitsteam das Netzwerk und die Endpunkte verteidigen kann.

Basic Security Suite

WebBlocker-URL-Filterung

WebBlocker blockiert automatisch bekannte bösartige Websites. Darüber hinaus können Sie mithilfe der differenzierten Inhalts- und URL-Filterungstools von WebBlocker unangemessene Inhalte sperren, die Netzwerkbandbreite beibehalten und die Produktivität Ihrer Mitarbeiter steigern.

spamBlocker

Spam wird in Echtzeit erkannt, bevor er massenhaft um sich greifen kann. Dabei ist spamBlocker ultra-schnell – und äußerst effektiv: Tagtäglich werden bis zu vier Milliarden Nachrichten überprüft.

Gateway AntiVirus (GAV)

Unsere Signaturen werden permanent aktualisiert und helfen Ihnen, bekannte Spyware, Viren, Trojaner, Würmer, Rogueware und Blended Threats zu ermitteln und zu sperren – einschließlich neuer Varianten bekannter Viren. Gleichzeitig verfolgt die heuristische Analyse verdächtiger Datenpakete und Aktionen, um zu verhindern, dass unbekannte Viren eindringen

Intrusion Prevention Service (IPS)

Mithilfe laufend aktualisierter Signaturen für die Überwachung des Datenverkehrs in allen gängigen Protokollen liefert IPS echtzeitbasierten Schutz vor Netzwerkbedrohungen, darunter Spyware, SQL-Injections, standortübergreifende Scripting-Angriffe und Pufferüberläufe.

Application Control

Mit dieser praktischen Funktion können Sie für Benutzer je nach Abteilung, Position im Unternehmen und Tageszeit den Zugriff auf Anwendungen gewähren, verweigern oder begrenzen. Anschließend verfolgen Sie in Echtzeit, was in Ihrem Netzwerk von wem aufgerufen wurde.

Reputation Enabled Defense Service (RED)

Ein leistungsstarker, cloudbasierter Reputations-Dienst, der Internetnutzer vor bösartigen Websites und Botnetzen schützt und dabei den Overhead bei der Webverarbeitung erheblich verbessert.

Network Discovery

Ein abonnementbasierter Dienst für Firebox®-Appliances, der eine visuelle Topologie sämtlicher Knoten in Ihrem Netzwerk generiert. So können Sie umgehend riskante Bereiche erkennen.

Zusätzliche Services in der Total Security Suite

APT Blocker

Dank Einsatz einer prämierten Sandbox der nächsten Generation erkennt und stoppt APT Blocker selbst raffinierte Attacken, einschließlich Ransomware, Zero-Day-Angriffe und andere hoch-entwickelte Malware.

Data Loss Prevention (DLP)

Dieser Dienst verhindert versehentlichen oder böswillig herbeigeführten Datenverlust, indem Texte und gängige Dateiarten in Bezug auf vertrauliche Inhalte analysiert werden. Dabei werden Versuche, sensible Informationen aus dem Netzwerk herauszuschleusen, sofort erkannt.

Threat Detection and Response

Setzen Sie Security-Events im Netzwerk und am Endpunkt mit detaillierten Analysen zur Bedrohungslage auf Enterprise-Niveau in Verbindung. Dadurch lassen sich potenzielle Angriffe noch früher erkennen und priorisieren. Sofortmaßnahmen zur Abwehr können rechtzeitig eingeleitet werden.

DNSWatch™

Durch die Erkennung und Behebung bedrohlicher DNS Anfragen werden Malware-Infektionen reduziert und User zu einer sicheren Seite mit Informationen und Anwendungsbeispielen weitergeleietet.

Access Portal*

Das WatchGuard Access Portal bietet einen zentralen Zugangspunkt für Cloud-gehostete Anwendungen und einen sicheren, clientlosen Zugriff auf interne Ressourcen über RDP und SSH.

Dimension Command

Dimension wandelt Logdaten von allen WatchGuard-Appliances in Ihrem Netzwerk in verwertbare Netzwerk- und Bedrohungsdaten um. Mit Dimension Command verwalten Sie alle Fireboxen über eine zentrale Konsole.

WatchGuard – Ein perfektes Team

So kaufen Sie die WatchGuard Security Services:

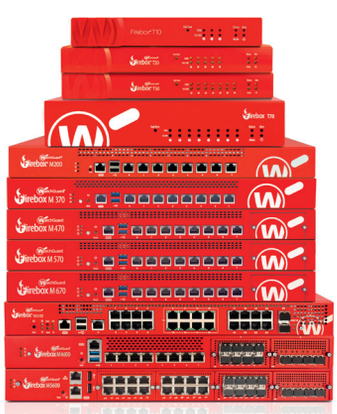
Um die hier beschriebenen Sicherheitsdienste nutzen zu können, benötigen Sie eine **WatchGuard Firewall/VPN Appliance.** Beim Kauf entscheiden Sie zunächst, ob Sie die „Basic Security Suite" oder die „Total Security Suite" lizensieren möchten. Ein späterer Umstieg von Basic auf Total ist zu jedem Zeitpunkt möglich. WatchGuard Firewalls, die zunächst nur mit „Standard Support" (ohne Security Services) gekauft wurden, können auch entsprechend nachlizensiert werden.

	Standard Support	Basic Security Suite	Total Security Suite
Stateful Firewall + VPN	Ja	Ja	Ja
WebBlocker		Ja	Ja
spamBlocker		Ja	Ja
Gateway Antivirus		Ja	Ja
Intrusion Prevention (IPS)		Ja	Ja
Application Control		Ja	Ja
RED + Botnet Detection		Ja	Ja
Network Discovery		Ja	Ja
APT Blocker			Ja
Data Loss Prevention (DLP)			Ja
Threat Detection & Response (TDR)			Ja
DNS Watch			Ja
Access Portal *			Ja
Intelligent Antivirus *			Ja
Dimension Command	optional	optional	Ja
Hersteller-Support	Standard (24x7)	Standard (24x7)	Gold (24x7)

* ab Firebox M370 aufwärts

So kaufen Sie eine WatchGuard Firewall/VPN Appliance:

Auf **www.boc.de/beratungstool** erhalten Sie anhand von ein paar Eckdaten eine erste Einschätzung, welches WatchGuard Modell für Ihre Anforderung in Frage kommt. Auf der zugehörigen Modellseite sehen Sie neben den Technischen Daten auch Preise für die verschiedenen Laufzeiten und Lizensierungsvarianten. Natürlich beraten wir Sie gerne auch persönlich. Nutzen Sie als Einstieg und bei Fragen gerne unser Kontaktformular, den Online-Chat auf **www.boc.d**e oder senden Sie eine E-Mail an **info@boc.de.**



Mit der WatchGuard Total Security Suite schneller zur DSGVO-Compliance

Abdeckung von 16 der Top 20 SANS-Sicherheitskontrollen (V6)

Die Top 20 SANS-Sicherheitskontrollen (v6)		
CS1	Inventarisierung autorisierter und nicht autorisierter Geräte	Ja
CS2	Inventarisierung autorisierter und nicht autorisierter Software	Ja
CS3	Sichere Hardware- und Softwarekonfigurationen auf Mobilgeräten, Laptops, Workstations und Servern	Ja
CS4	Kontinuierliche Bewertung und Behebung von Schwachstellen	Ja
CS5	Kontrollierte Nutzung von Administratorrechten	Ja
CS6	Verwaltung, Monitoring und Analyse von Prüfprotokollen	Ja
CS7	Schutz für E-Mail und Webbrowser	Ja
CS8	Schutz vor Malware	Ja
CS9	Einschränkung und Kontrolle von Netzwerkports, -protokollen und -diensten	Ja
CS10	Möglichkeit zur Wiederherstellung von Daten	Nein
CS11	Sichere Konfiguration für Netzwerkgeräte wie Firewalls, Router und Switches	Ja
CS12	Absicherung des Netzwerkperimeters	Ja
CS13	Datenschutz	Ja
CS14	Kontrollierter Zugriff basierend auf dem Need-to-know-Prinzip	Ja
CS15	Kontrolle drahtlosen Zugangs	Ja
CS16	Kontenüberwachung und -kontrolle	Ja
CS17	Bewertung der Sicherheitskompetenzen und angemessene Schulungen zum Schließen von Lücken	Nein
CS18	Sicherheit der Anwendungssoftware	Ja
CS19	Ereignisabhängige Reaktion auf Eingriff	Nein
CS20	Penetrationstest und Red-Team-Übungen	Nein

WatchGuard®

SCHÜTZEN SIE IHR UNTERNEHMEN • SCHÜTZEN SIE IHRE RESSOURCEN • SCHÜTZEN SIE IHRE MITARBEITER

WatchGuard ist seit 22 Jahren Wegbereiter bei der Entwicklung innovativer Cybersicherheits-Technologie und stellt sie in einer benutzer- und verwaltungsfreundlichen Lösung bereit. Durch branchenführende Netzwerksicherheit, sicheres WLAN sowie Produkte und Dienstleistungen im Bereich der Network Intelligence ermöglicht WatchGuard über 80.000 Kunden weltweit den Schutz ihrer wichtigsten Ressourcen – in einer Welt, in der die Zahl neuer Bedrohungen in der Cybersicherheits-Landschaft tagtäglich wächst.

Auch kleine und mittelständische Unternehmen fallen Angriffen, die schwerwiegende Auswirkung auf betriebliche Vorgänge und auf die Geschäftskontinuität haben, immer noch zum Opfer. WatchGuard bietet Ihnen den erforderlichen mehrschichtigen Schutz vor Malware und macht Ihnen die Verwaltung leicht. Ihr Unternehmen ist den gleichen Bedrohungen ausgesetzt wie ein Großunternehmen. Sollten Sie dann nicht auch vom gleichen Sicherheitsniveau profitieren?

b.o.c. IT-SECURITY

Künzeller Straße 93 · D-36043 Fulda
Telefon: +49 661 9440440
E-Mail: info@boc.de · www.boc.de

Erfolg durch Spezialisierung: Die BOC IT-Security GmbH vertreibt und betreut ausschließlich IT-Security Lösungen des Herstellers WatchGuard: Hardware Firewall/VPN Appliances, Mobile User Access und Wireless Infrastructure. Seit nunmehr 20 Jahren arbeiten wir täglich mit diesen Produkten. Kompetenz und Know-How zeichnen uns als Partner für WatchGuard-Installationen egal welcher Größenordnung aus. Wir sind gerne deutschlandweit für Sie da.

Auf unserer Website www.boc.de finden Sie umfangreiche Produktinformationen und Preise zu WatchGuard-Produkten. In unserem kostenfreien WatchGuard Infoportal bieten wir Ihnen zahlreiche HOWTO-Artikel und unseren Technischen Blog.

Wenn Sie diese Broschüre hilfreich finden und in Ihrem Unternehmen an Kollegen weiterverteilen möchten, wenden Sie sich bitte an uns. Bis 10 weitere Exemplare stellen wir Ihnen gerne kostenfrei zur Verfügung, darüber hinaus zum Selbstkostenpreis.