SONICWALL®

DIE SCHATTENSEITE DER VERSCHLÜSSELUNG

Hacker entwickeln ihre Fähigkeiten ständig weiter. Mittlerweile nutzen sie SSL-Datenverkehr, um ihre Malware und ihre Angriffe vor Sicherheitssystemen zu verbergen.

97 % der befragten Unternehmen haben eine Zunahme des verschlüsselten Webverkehrs beobachtet[1]

130%ige Zunahme von Bedrohungen in 2016, die TLS-/SSL-Verbindungen nutzen (gegenüber 2014)[1]

80 % der Befragten waren schon einmal Opfer eines Cyberangriffs[2]

41 % der Angriffe verbargen sich im SSL-Verkehr[2]

[1] *Studie, NSS Labs, Juni 2016*
[2] *Studie, Ponemon-Studie 2016*

SONICWALL®

Angriffe, die SSL-Verkehr nutzen, um eine Erkennung zu vermeiden

Angriffe, die sich im „normalen“ Port-443-Datenverkehr verstecken

- 78 Prozent der Befragten meinen, dass ihre Organisation wahrscheinlich im Visier von Angreifern steht.
- Weniger als ein Drittel (30 %) der Organisationen war der Ansicht, diesem Problem gewachsen zu sein.

Phishing

- 79 Prozent glauben, dass die Wahrscheinlichkeit eines Phishing-Angriffs in ihrer Organisation sehr hoch ist.
- Nur 17 Prozent behaupten, dass ihre Organisation in der Lage ist, solche Attacken abzuwehren.

Malware, die sich in ausgehenden Daten innerhalb von verschlüsseltem Datenverkehr verbirgt

- 74 Prozent geben zu, dass dieser Angriffsvektor sehr wahrscheinlich ist.
- Nur 16 Prozent meinen, dass ihre Organisation SSL-verschlüsselte Malware-Angriffe vor dem Herausschleusen von Daten identifizieren und verhindern könne.

Angreifer könnten ausgehende und/oder gestohlene Daten unbemerkt an einen Command-and-control-Server übertragen.

- 66 Prozent geben an, dass die Wahrscheinlichkeit eines solchen Vorfalls sehr groß ist.
- 26 Prozent glauben, dass ihre Organisation ein solches Verhalten identifizieren und Datenverlust verhindern könne.

Studie, Ponemon-Studie 2016

So machen sich Hacker die Verschlüsselung zunutze

Seitenanforderung: Nutzer (Opfer A) ruft auf seinem Rechner eine unbedenkliche Website auf, die aber bösartigen Code enthält.

Ausführung des Exploit-Kits: Bei der Übertragung des Webinhalts an den Client wird ein kleines Softwareprogramm auf das Gerät des Benutzers heruntergeladen. Anschließend wird eine Abfolge von Befehlen ausgeführt, um die Software-Schwachstellen auf dem Client-Gerät auszunutzen.

Malware-Anfrage: Sobald der Betreiber des Exploits-Kits das Gerät unter seiner Kontrolle hat, wird ein Request-Befehl an eine Website gesendet, die Malware hostet und bereitstellt.

Infektion mit Malware: Auf dem Rechner von Opfer A ist nun Malware installiert.

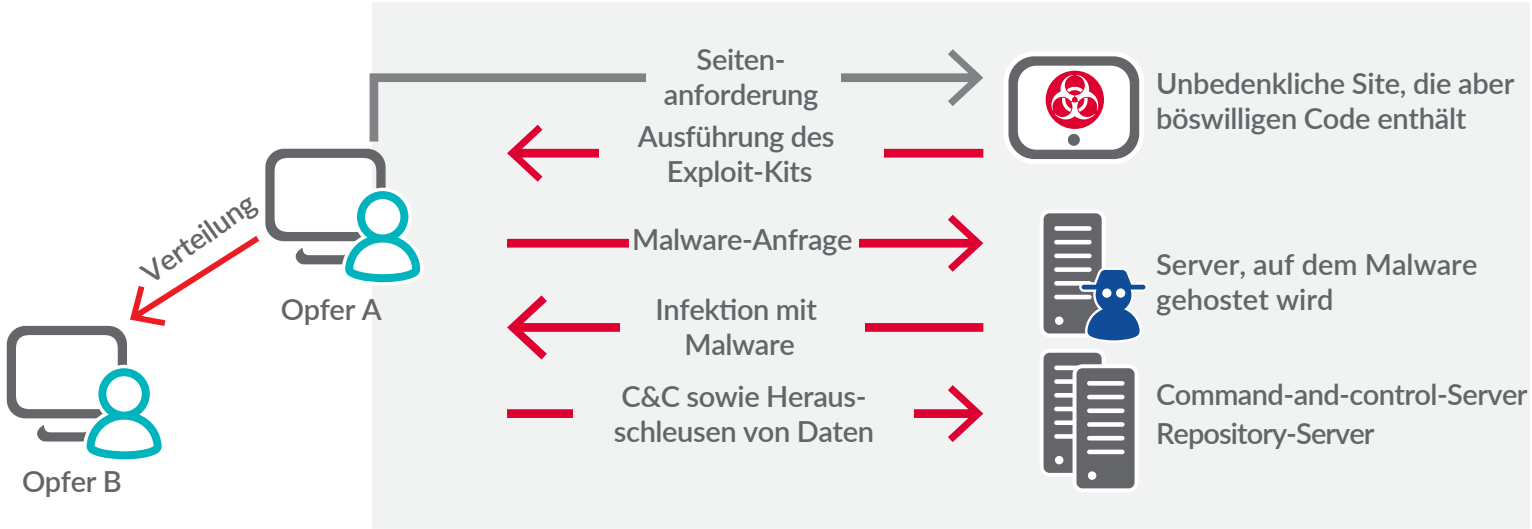
C&C: Die Malware kommuniziert mit einer Command-and-control-Infrastruktur, um weitere Anweisungen zu erhalten.

Herausschleusen von Daten: Daten auf dem Rechner von Opfer A werden zur Verarbeitung auf einen externen Server kopiert.

Opfer B: In dieser Phase erweitern Angreifer oft ihre Zugriffsrechte, sodass sie sich innerhalb des Netzwerks „seitlich“ ausbreiten und weitere Endpunkte infizieren können.

Verschlüsselung: Neu daran ist, dass sich die Verschlüsselung in jeder Phase dieses Angriffs nutzen lässt, um eine Erkennung zu vermeiden.

Die Verschlüsselung lässt sich in jeder Phase eines Angriffs nutzen



SONICWALL®

Drei typische Hürden, die einer Prüfung des SSL-Verkehrs im Wege stehen

Mangel an geeigneten Sicherheitstools

unzureichende Ressourcen

Leistungseinbußen

Quelle: Studie, Ponemon-Studie 2016

SONICWALL®

Die Beeinträchtigung der Performance ist ein großes Problem

- **61 Prozent** der Befragten entschlüsseln den SSL-Verkehr nicht, weil sie Leistungseinbußen befürchten*

- **83 Prozent** sagen, dass es in Organisationen, die den SSL-Verkehr entschlüsseln und prüfen, in irgendeiner Form zu Beeinträchtigungen kommt*

*Quelle: Studie, Ponemon-Studie 2016

SONICWALL®

Stellen Sie kritische Fragen

- Wissen Sie, ob Ihre Firewall HTTPS-Datenverkehr überprüft?

- Hatte Ihre Organisation häufig mit Netzwerkunterbrechungen oder -ausfällen zu kämpfen, weil die Performance Ihrer Firewall bei der Prüfung von HTTPS-Verkehr komplett zusammengebrochen ist?

- Wie skalieren Sie die Firewall-Schutzfunktionen, um Leistungseinbußen, Verzögerungen und Latenzprobleme Ihres Netzwerks bei der Prüfung von HTTPS-Verkehr zu verhindern?

Empfehlungen

- Falls Sie schon seit längerem keinen Sicherheitsaudit mehr durchgeführt haben, sollten Sie jetzt eine umfassende Evaluierung Ihrer Netzwerksicherheit vornehmen, um Ihre Risiken und Bedürfnisse zu identifizieren.

- Aktualisieren Sie Ihre Sicherheitsregeln, um sich vor einer größeren Bandbreite an Bedrohungsvektoren zu schützen. Richten Sie mehrere Sicherheitsmechanismen gegen Angriffe – egal ob im HTTP- oder HTTPS-Verkehr – ein.

- Implementieren Sie eine Next-Generation-Firewall mit leistungsstarker SSL-/TLS-Prüffunktion (Secure Sockets Layer/ Transport Layer Security). Stellen Sie sicher, dass Sie sämtlichen Datenverkehr unabhängig von Port, Protokoll oder Dateityp überprüfen. Ihr System sollte auch jedes einzelne Paket entpacken und entschlüsseln und jedes einzelne Byte untersuchen, um Bedrohungen schnell zu identifizieren.

- Standard-Sandboxing-Lösungen sind nicht in der Lage, Malware aufzuspüren, die sich in verschlüsseltem Datenverkehr verbirgt. Neben Funktionen zur SSL-/TLS-Prüfung benötigen Sie auch eine Netzwerk-Sandbox, die den Datenverkehr bis zur Klärung des Sicherheitsstatus blockiert und Zero-Day-Angriffe nicht nur erkennt, sondern auf automatisierte Weise verhindert.

- Darüber hinaus sollten Sie Content-Filtering-Funktionen hinzufügen, um zu verhindern, dass Nutzer fragwürdige Websites besuchen. Nutzen Sie auch ein Gateway-Anti-Virus- und Intrusion-Prevention-System, um Ihre User vor eigentlich unbedenklichen Websites zu schützen, die aber kompromittiert wurden.

- Machen Sie Ihre Mitarbeiter immer wieder auf die Gefahren von Social Media, Social Engineering, verdächtigen Websites und Downloads sowie verschiedenen Spam- und Phishingmails aufmerksam. Insbesondere sollten Sie Ihren Usern nahelegen, dass sie unter keinen Umständen selbst signierte, ungültige Zertifikate akzeptieren sollten.

- Achten Sie auf optimale Praktiken im Cyberspace. Zum Beispiel sollten Sie sicherstellen, dass Ihre ganze Software über die aktuellen Sicherheitsupdates verfügt. Auf diese Weise können Sie all Ihre Geräte vor älteren SSL-Exploits schützen, die bereits neutralisiert wurden.

- Erstellen Sie einen Plan für die Reaktion auf bzw. die Behebung von Problemen und gehen Sie ihn sorgfältig durch. Testen Sie Ihren Plan regelmäßig, führen Sie Simulationen wie bei einer Brandschutzübung durch, verbessern Sie den Prozess und sorgen Sie dafür, dass die „Mitarbeiter an vorderster Front“ die nötige Schulung erhalten, um effizienter zu arbeiten und die Pläne zur Fehlerbehebung wie vorgesehen auszuführen.

Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:
SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com