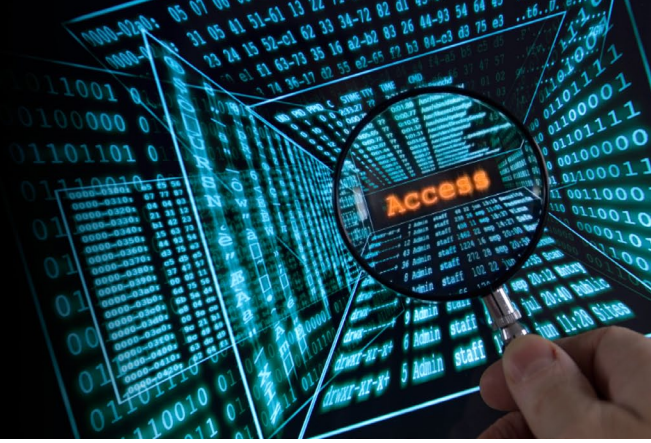
Netop



Fernzugriffs-Sicherheit

Wie wichtig ist das Thema? Was können Sie tun?

Im März 2013 berichteten ZDNet, Computerworld und andere Medien, dass eine beliebte und sehr bekannte Fernzugriffslösung von einer Gruppe von Hackern kompromittiert wurde, um „Aktivisten und Ziele im Industrie-, Forschungs- sowie im diplomatischen Bereich anzugreifen“ [1]. Bei den Angriffen wurde Malware installiert, deren Zweck darin bestand, Bildschirmfotos zu machen, Informationen über die Systeme und lokalen Benutzerkonten zu sammeln und die Festplatten nach bestimmten Dateitypen abzusuchen.

Derartige Vorfälle häufen sich leider: Fast jede Woche hören wir von einer anderen Organisation, die irgendeiner Art von Cyberkriminalität zum Opfer fällt – Betrug, Diebstahl oder Hacking. Im Jahr 2012 führte die weltweite Vernetzung von Rechnern, Geräten, Personen und Netzwerken zu 900 gemeldeten Fällen von Diebstahl oder Datenverlust, wobei allein in sechs Fällen insgesamt beinahe 40 Millionen Datensätze kompromittiert wurden [2]. Trotz zahlreicher Warnungen, umfassender Berichterstattung in den Medien und dem Einsatz von Sicherheitsrichtlinien kämpfen Unternehmen nach wie vor mit Cyberbedrohungen.

Noch komplizierter wird die Situation durch die schiere Anzahl von existierenden Verbindungen. Von Smartphones, Tablets und Laptops bis hin zu Geldautomaten, Serverfarmen und Gebäudesensoren sind die meisten Geräte heutzutage mit dem Internet verbunden. Ungeschützt bietet jedes von ihnen Hackern eine Angriffsmöglichkeit, was zu erheblichen Schäden führen kann.

Bei der Nutzung eines Dienstes wie Shodan – einer Art Suchmaschine, mit der man Geräte finden kann, die mit dem Internet verbunden sind – haben Hacker beispielsweise Zugriff auf eine wahre Fundgrube von Informationen über potenzielle Sicherheitsschwächen. Mithilfe kostenlos erhältlicher Fernzugriffs-Software können sie die betreffenden Geräte dann attackieren. Fernzugriffslösungen bieten Geschäftsvorteile von unschätzbarem Wert, aber die bedauerliche Tatsache ist, dass 88 % [3] aller Hackerangriffe anhand von Fernzugriffs-Tools durchgeführt werden.

Das Team hinter diesen Attacken war seit 2008 aktiv. Vermutlich bereits seit 2004. Sie instrumentalisierten dabei eine - mit über 100 Millionen Anwendern - weithin verwendete Remote Control-Anwendung. Trotz gültiger digitaler Zertifikate gelang es ihnen Aktivisten, Politiker, Geheimdienste, sowie die Energie- und Schwerindustrie anzugreifen.

- KASPERSKY LAB REPORT, VERSION 1.02, MÄRZ 2013

BEMERKENSWERTE HACKING-VORFÄLLE

JAHR	UNTERNEHMEN	BETROFFENE DATENSÄTZE
2012	Zappos	24.000.000
2011	Sony Corporation	77.000.000
2011	SK Communications	35.000.000
2009	Heartland Payment Systems	130.000.000
2009	RockYou, Inc.	35.000.000
2007	TJX Companies	94.000.000

Quelle: DataLossDB.org - www.datalossdb.org

Mit dem richtigen Know-how, Geduld und einigen Internetsuchen können Hacker Schwachstellen ausnutzen – von praktisch jedem Ort der Welt aus. Und während die Anzahl von verbundenen Geräten permanent zunimmt, gilt dasselbe für die Gelegenheiten für Cyberverbrechen.

Wie also kann eine Organisation sicherstellen, dass sie bei der Nutzung einer Fernzugriffslösung alle nötigen Vorsichtsmaßnahmen ergreift?

Der Schlüssel ist die Verwendung eines mehrstufigen Modells, bei dem die Sicherheit die größte Rolle spielt. Als erstes sollten angemessene Schulungen und Verfahren für Mitarbeiter eingeführt werden. In vielen Branchen bieten Compliance-Vorschriften wie HIPAA und PCI hilfreiche Rahmenbedingungen, welche auch spezifische Richtlinien für Fernzugriff umfassen.

Neben der Durchsetzung solcher Richtlinien können Unternehmen auch in Lösungen wie Netop Remote Control investieren. Netop bietet seit fast 30 Jahren sicheren Fernzugriff. Im Gegensatz zu einigen anderen bekannten Fernzugriffslösungen – die für Hacker frei verfügbar sind – bietet Netop keine kostenlose Lösung für Einzelpersonen an. Durch die alleinige Konzentration auf Unternehmenslösungen und bestimmte Kunden wird die Gefahr eines Missbrauchs der Lösung von Netop im Rahmen von Cyberangriffen minimiert.

Außerdem bietet Netop von Grund auf integrierte, mehrstufige Sicherheitsfunktionen, die nicht nur Mitarbeitern bei der Einhaltung von Unternehmensrichtlinien helfen, sondern auch das Maß an Sicherheit maximieren, wenn zwei oder mehr Geräte verbunden sind oder versuchen, eine Verbindung herzustellen.

Netop Remote Control hilft Organisationen durch:

Sicherung der Verbindung

Mit Netop können Unternehmen internetbasierten Fernzugriff über ihre eigenen Server bereitstellen, was vollständige Transparenz und Kontrolle sowie eine lückenlose Einhaltung von unternehmensweiten Sicherheitsrichtlinien ermöglicht. Organisationen können hierarchische Verbindungs-Accounts zentral verwalten und genau festlegen, wer worauf zugreifen kann – sogar schon vor Beginn des Authentifizierungsvorgangs. Auf diese Weise haben Unternehmen vollständige Kontrolle über ihre eigenen Daten und die Sicherheit.

Außerdem bietet Netop zusätzliche sichere Verbindungsoptionen – einschließlich einer von Netop gehosteten Version; in allen Fällen jedoch wird der Fernzugriffs-Datenverkehr anhand von marktführender 256-Bit-AES-Verschlüsselung und dynamischem Schlüsselaustausch per Diffie-Hellman-Methode mit Schlüssellängen bis zu 2048 Bit gesichert, um Ihr Unternehmen und Ihre Daten zu schützen.

Verwaltung des Benutzerzugriffs

Das Zielgerät muss bestimmte Kriterien für das Akzeptieren von eingehenden Einladungen vorgeben, da ansonsten jeder Eindringling anhand von unbefugten Einladungen Zugriff auf Ihr Netzwerk nehmen könnte. Bei der Verwaltung der Zugriffsrechte von Benutzern werden die Kriterien festgelegt, aufgrund derer der das Zielgerät Einladungen annehmen sollte.

Mit Netop sind zu diesem Zweck Kombinationen der folgenden Maßnahmen möglich:

- MAC/IP-Adressprüfung. Zielgeräte akzeptieren nur Anfragen von Mitarbeitern, deren Adresse auf einer zuvor definierten MAC/IP-Liste enthalten ist.
- Geschlossene Benutzergruppen. Sie können allen Service-Mitarbeitern und Zielgeräten Seriennummern zuweisen, um nur Verbindungen zwischen bestimmten Nummern zu ermöglichen. Service-Mitarbeiter mit anderen Seriennummern werden abgelehnt.

Welches sind die potenziellen Schäden von Hacker-Angriffen?

- Verlust von Daten/ Geschäftsgeheimnissen.
- Verlust von Kundendinformationen, einschließlich Kreditkartendaten.
- Millionen Fälle von betrügerischer Nutzung.
- Ein PR-Alptraum *

* Ein Netop Kunde, ein großer Versorgungsbetrieb, schätzte die Kosten in Verbindung mit den potenziellen Schäden durch eine Sicherheitsverletzung auf 10 Millionen USD. Bedenkt man jedoch, dass der Vorfall bei TJX im Jahr 2007 das Unternehmen mehr als 64 Millionen USD kostete, wirkt diese Schätzung zu vorsichtig.

Medienberichte über Hacking-Angriffe mithilfe von Fernzugriffslösungen

Hacker nutzen legales IT-Fernsupport-Tool bei Spyware-Angriff

- ZDNET, MÄRZ 2013

Zwei Anklagen im Zusammenhang mit dem Diebstahl von 40.000 USD über gehackte POS-Terminals in Subway-Restaurants

- CNET, MÄRZ 2013

Wie Hacker Subway eine 3-Millionen-Dollar-Lektion in Sachen POS-Sicherheit erteilten

- ARS TECHNICA, DEZEMBER 2011

- Authentifizierung. Netop Remote Control lässt sich in die Authentifizierungsmethode integrieren, die Kunden für ihre Netzwerke verwenden – egal ob die Authentifizierung per Windows Domain, Verzeichnisdienst, RADIUS-Server oder RSA SecurID-Server erfolgt.

- Callback. Ein Zielgerät kann einen Mitarbeiter anhand einer Modem-, ISDN- oder TCP-Verbindung zurückrufen. Dafür muss sich der Mitarbeiter an einem bestimmten Ort oder Rechner befinden, was für Eindringlinge ein weiteres Hindernis darstellt.

- Benutzergesteuerter Zugriff. Bei Verwendung dieser Funktion erscheint ein Popupfenster auf dem Zielgerät, das die ID des Service-Mitarbeiters enthält und den Endbenutzer fragt, ob er eine eingehende Verbindung akzeptieren möchte. Eine Fernsupport-Sitzung kann nur hergestellt werden, wenn der Endbenutzer sie genehmigt.

Verwaltung der Benutzerrechte

Unterschiedliche Fernzugriffsnutzer benötigen unterschiedliche Zugriffsprofile. Unternehmen sollten in der Lage sein, die Funktionalität für Benutzer nach Bedarf anzupassen: Tastatur und Maus sperren, Bildschirme verdunkeln, bestimmte Befehle ausführen, Dateien übertragen, Programme ausführen, Dienste verwalten, Eingabeaufforderungen durchführen, die Registry bearbeiten usw.

Einige High-End-Fernsteuerungsprodukte ermöglichen Organisationen zwar die Verwaltung von Benutzerrechten, aber nicht alle bieten eine zentralisierte Verwaltung. Mit Netop kann ein Unternehmen die Einstellungen für tausende von Computern ändern, ohne jedes Gerät einzeln konfigurieren zu müssen.

Aktivitäten dokumentieren

Netop kann Prüfpfade sowohl für unseren gehosteten als auch für den von Kunden gehosteten Verbindungsdienst zur Verfügung stellen, was eine Rückverfolgung und Auditierung aller Aktivitäten ermöglicht. Dokumentation ist der letzte Pfeiler eines stabilen, sicheren Fernsteuerungssystems. Wenn alle Sitzungen protokolliert und Videoaufzeichnungen von ihnen erstellt werden, wissen Sie stets genau, was passiert ist und wann es passiert ist. Hat der Servicedesk-Mitarbeiter die wichtige Vertriebsdatei gelöscht, während er sich um das Internetproblem des Verkäufers kümmerte? Wer hat am Samstagabend Fernzugriff auf die vertraulichen Krankenakten genommen? Dies sind Fragen, die Unternehmen beantworten können müssen, und Netop ermöglicht es ihnen.

Fazit

Cyberbedrohungen sind überall und die Auswirkungen von Sicherheitsverletzungen können erhebliche Schäden verursachen. Aufgrund der permanent steigenden Anzahl von Geräten und Verbindungen und der Anzahl von Tools, die Hacker für ihre Zwecke nutzen können – von Shodan bis hin zu beliebten und leicht zugänglichen Fernzugriffs-Tools – nehmen die Gelegenheiten für kriminelle Handlungen kontinuierlich zu. Unternehmen können sich jedoch wehren, indem sie strenge Sicherheitsrichtlinien durchsetzen und in eine sichere Fernzugriffslösung wie Netop Remote Control investieren.

QUELLEN

1. Hacker nutzen legales IT-Fernsupport-Tool bei Spyware-Angriff

http://www.zdnet.com/hackers-use-legit-remote-it-support-tool-in-spy-attack-7000012949/

2. DataLossDb.org

http://www.datalossdeb.org

3. Verizon 2012 Data Breach Investigations Report

http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?__ct_return=1

4. Kaspersky Lab Report

http://www.securelist.com/en/downloads/vlpdfs/theteamspystory_final_t2.pdf

Netop

Netop entwickelt und verkauft marktführende Software-Lösungen, die einen raschen, sicheren und nahtlosen Transfer von Video- und Audiomaterial, Bildschirminhalten und anderen Daten zwischen zwei oder mehr Computern ermöglichen.

Für weitere Informationen besuchen Sie: www.netop.com