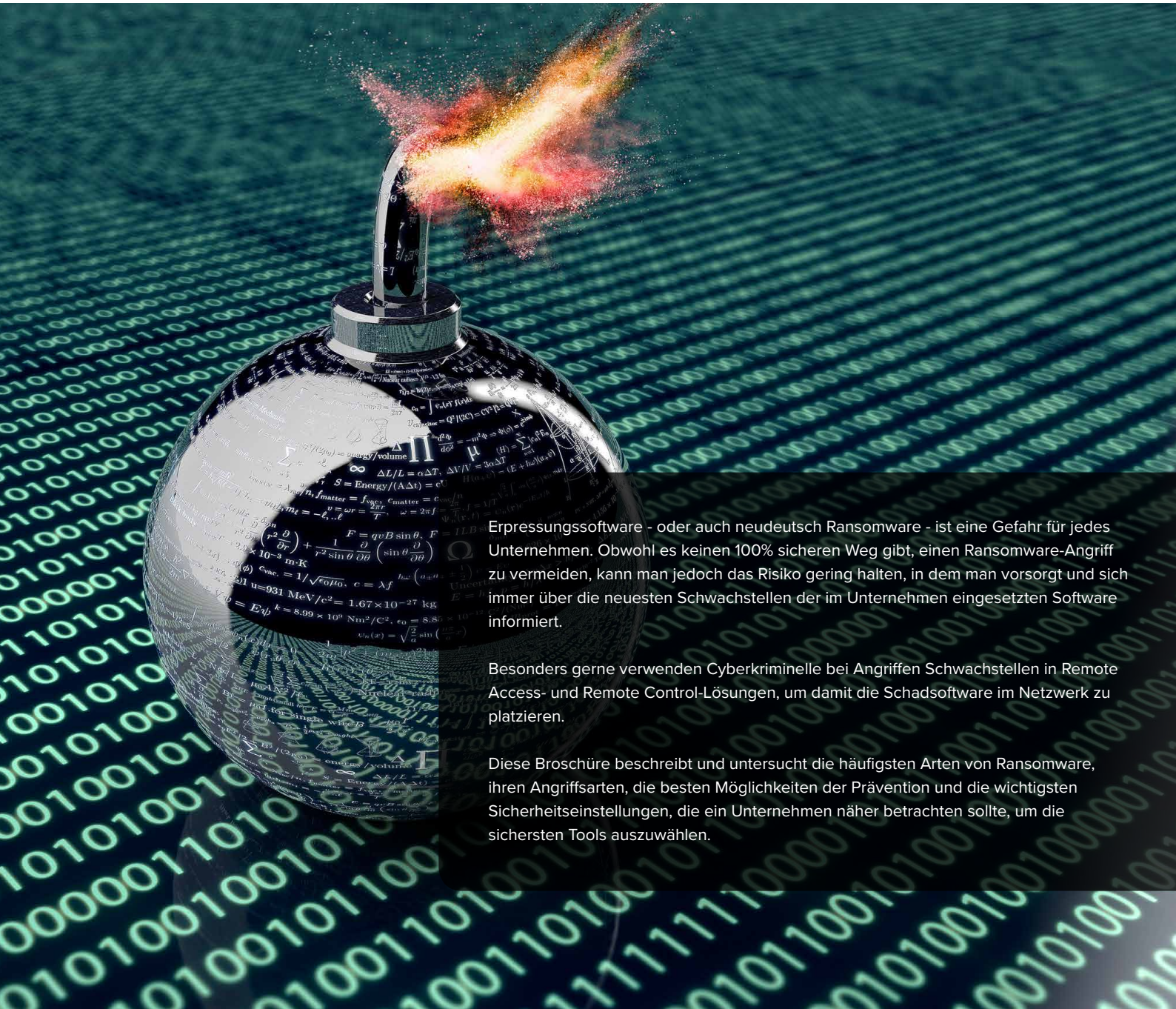
SICHERHEITSINFORMATIONEN

NETOP® Remote Control

Schützen Sie Ihre Daten vor Erpressungssoftware



Erpressungssoftware - oder auch neudeutsch Ransomware - ist eine Gefahr für jedes Unternehmen. Obwohl es keinen 100% sicheren Weg gibt, einen Ransomware-Angriff zu vermeiden, kann man jedoch das Risiko gering halten, in dem man vorsorgt und sich immer über die neuesten Schwachstellen der im Unternehmen eingesetzten Software informiert.

Besonders gerne verwenden Cyberkriminelle bei Angriffen Schwachstellen in Remote Access- und Remote Control-Lösungen, um damit die Schadsoftware im Netzwerk zu platzieren.

Diese Broschüre beschreibt und untersucht die häufigsten Arten von Ransomware, ihren Angriffsarten, die besten Möglichkeiten der Prävention und die wichtigsten Sicherheitseinstellungen, die ein Unternehmen näher betrachten sollte, um die sichersten Tools auszuwählen.

Übersicht: Remote Access & Ransomware

2016 wurde gerade erst zum „Jahr der Erpressungssoftware“ gekürt. Dies hat es der großen Anzahl gerade dieser Cyber-Attacken zu verdanken. Diese hartnäckige Bedrohung macht aktuell kleinen Unternehmen zu schaffen, wie auch weltweiten Konzernen. IT-Dienstleister, staatliche Behörden, Handelshäuser, das Gesundheitswesen, Universitäten und Finanzinstitute sind prädestinierte Zielgruppen für Ransomware. Cyberkriminelle suchen ganz gezielt nach Schwachstellen in Softwareprodukten. Hier ist die Wahrscheinlichkeit, Erpressungsgelder zu erhalten, am größten. Wurde eine Schwachstelle in einer Software, die von vielen Unternehmen genutzt wird, entdeckt, kommt es zu regelrechten Wellen von Attacken auf diese Schwachstelle.

Zuletzt entdeckten Cyberkriminelle, dass Schwachstellen in weit verbreiteten Remote-Access Tools, wie z.B. RDP, genutzt werden können, um Schadsoftware einzuschleusen. Viele Unternehmen tragen heutzutage ein hohes Risiko eines Ransomware-Angriffs.

Hauptgrund: eine unübersichtliche Fülle an eingesetzten Remote-Access Tools. Auch heute noch findet man eine große Anzahl vertraulicher Daten, wie personenbezogene Daten, geistiges Eigentum und Finanzinformationen, die für Ransomware Angriffe geradezu offen zugänglich sind. Die betroffenen Unternehmen verwenden Remote-Access Tools ohne adäquate Sicherheitsfunktionen. Selbst nach Rückgabe der Daten können sich die rechtmäßigen Besitzer nicht sicher sein, dass die Daten kopiert und im Darknet weitervertrieben werden.

Fox-IT erklärt, warum gerade Remote-Access Server beliebte Ziele für Ransomware wurden: „Ihr Vorteil liegt in der Zeit, die die Angreifer unentdeckt bleiben können, wenn keine wirksamen Ortungssysteme vorhanden sind. Nur zum Beispiel: Die Angreifer haben genug Zeit zu analysieren, wie und wann Backups von wichtigen Daten erstellt werden, bevor sie die Ransomware einsetzen. So können sie sicherstellen, dass die Backups im Nachhinein nicht verwendet werden können, um die verschlüsselten Daten wiederherzustellen. Die Angreifer erhöhen damit die Wahrscheinlichkeit, Lösegeld vom Unternehmen erpressen zu können.“ (lindagerrits, 2016)

Bevor wir uns den effektivsten Methoden zuwenden, um die Gefahren eines Angriffs zu minimieren und die Daten Ihres Unternehmens oder Ihrer Kunden zu schützen, sollten wir uns zunächst die verschiedenen Arten von Ransomware genauer ansehen.

Was ist Ransomware?

Ransomware ist eine Schadsoftware, die sich unbemerkt auf dem Computer eines Opfers installiert. Als Folge wird dem Opfer der Zugang zu seinem eigenen Betriebssystem versperrt. Es wird dann ein Lösegeld eingefordert, das bei Zahlung dem Opfer den Zugang wieder gewährt.

Warum ist ein Ransomware Angriff so gefährlich? Zuallererst kann der Angreifer natürlich auf vertrauliche Daten zugreifen und diese auch unter Umständen zerstören. Dieser Angriff kann zu finanziellen Verlusten führen und ganze Prozesse im Unternehmen zum Erliegen bringen. Je nach dem, wie sich ein Unternehmen auf diese Gefahr vorbereitet hat und in der Lage ist, darauf zu reagieren, kann der Ruf eines Unternehmens dadurch nachhaltig geschädigt werden.

Arten von Ransomware

Es gibt derzeit zwei gängige Arten von Ransomware:

1. **Locker Ransomware (nicht verschlüsselnd)**
   Der Anwender kann seinen Rechner nicht mehr vernünftig bedienen. Üblicherweise erscheint ein Fenster, das nicht mehr geschlossen werden kann, mit einer Lösegeldforderung. Erst nach Zahlung lässt sich dieses Fenster beenden..
2. **Verschlüsselnde Ransomware (Kryptoware)**
   Diese Art der Schadsoftware verschlüsselt die Ordner eines Anwenders. In manchen Fällen sogar die gesamte Festplatte oder auch die Master File Tabelle, um die Daten unzugänglich zu machen.

Die Angriffsarten

Immer neue Angriffsarten von Ransomware werden entdeckt. Es ist wichtig zu verstehen, wie die Cyberkriminellen Zugang zu den Systemen ihrer Opfer erhalten. Nur so können Sie die richtigen Vorsorgemaßnahmen treffen und einen Angriff verhindern.

Die geläufigsten Methoden der Kriminellen, einen Angriff zu starten:

- Spam und Social Engeneering
- Direkter Drive-by-Download oder auch Schad-Werbung
- Ausnutzen von Schwachstellen in Programmen wie RDP, VNC oder Teamviewer
- Weiterleiten des Internetverkehrs auf schädliche Websites
- Partner-Systeme/ Ransomware-as-a-service (RaaS)
- Einfügen von schädlichem Code in zuverlässigen Webseiten
- Schadsoftware-Installations-Tools und Botnets
- SMS Nachrichten (Ransomware, die auf Mobilgeräte abzielen)
- Verbreitung von einem infizierten Computer zum nächsten

Nachdem die Schadsoftware in einen Computer eingedrungen ist, bleibt sie zunächst inaktiv und wiegt das Opfer in vermeidlicher Sicherheit. Stunden oder Tage später verschlüsselt die Schadsoftware dann so viele Daten wie nur möglich. Manche Angreifer fügen den übernommenen Computer auch noch zu einem Botnet hinzu, um von dort aus weitere Systeme anzugreifen.

Dem Anwender wird nun so lange der Zugriff auf seine Daten versperrt, bis die Lösegeldforderungen erfüllt werden. Die Angreifer geben eine nicht zurückverfolgbare E-Mail-Adresse an mit Anweisung, ein Lösegeld z.B. in Bitcoins zu bezahlen.

Auf wen wird abgezielt?

Cyberkriminelle suchen sich vor allem Organisationen, die entweder bewusst oder unbewusst die notwendigen Sicherheitsstandards vernachlässigen. Erstaunlicherweise betrifft dies einen Großteil aller Unternehmen. Unternehmen, die Tools und Programme nutzen, die bekannte Schwachstellen haben, wie z.B. ungeschützte Remote Desktop Server, sind Hauptaugenmerk für diese Schadsoftware überhaupt.

Öffentliche Einrichtungen wie Krankenhäuser, Polizei, Schulen und das Rettungswesen sind beliebte Ziele. Ein Ausfall von Systemen ist hier besonders kritisch. Sie sind geradezu gezwungen, die geforderten Summen sofort zu zahlen, um den Betrieb zu gewährleisten.

Der Ablauf eines verschlüsselnden Ransomware-Angriffs

Um sich und eigene Kunden zu schützen, müssen Sicherheitsbeauftragte und Administratoren Kenntnis über den Ablauf eines Ransom-Angriffs erhalten, der die Systeme infiziert und sich zudem im Netzwerk verbreitet:

Phase 1: Installation

1. Der Nutzer besucht eine infizierte Website oder wurde von einem Angreifer getäuscht.
2. Der Nutzer erhält einen Anhang oder Link zu einer Datei. Die Schadsoftware wird heruntergeladen und der Angreifer sucht eine Schwachstelle im System des Opfers.

   Beispielsweise vertrauen viele Unternehmen der Remote-Desktop Funktionalität und Cyberkriminelle nutzen dann RDP, um verschlüsselnde Ransomware-Angriffe zu starten. Häufig genug geschieht dies über Brute-Force-Angriffe oder auf dem Schwarzmarkt zugekaufte Zugangscodes. Damit verschaffen die Kriminellen sich Zugang zu den Systemen und können nun manuell die Schadsoftware auf dem Computer des Opfers installieren.
3. Die eigentliche Verschlüsselungssoftware wird ausgepackt und installiert sich auf dem infizierten Computer (oder „Bot“).

Phase 2: Infektion & Verbreitung

4. Die Schadsoftware kontaktiert den Command- und Control-Server (C&C Server) des Kriminellen und erhält den Kodierungsschlüssel und gegebenenfalls weitere Anweisungen.
5. Das infizierte System wird als Startplattform genutzt, um die Schadsoftware im Netzwerk zu verbreiten. Die Ransomware bleibt jedoch inaktiv, bis die Angreifer die gewünschte Anzahl an infizierten Bot-Netz-Rechner erreicht haben. Dann erfolgt die Auslieferung der öffentlichen Schlüssel vom C&C Server an die Bots.

Phase 3: Verschlüsselung und Erpressung

6. Die Ransomware verschlüsselt den gesamten Inhalt der Festplatte mithilfe einer RSA-2048-Verschlüsselung. Die verschlüsselten Daten werden dann über den Terminal-Services-Client Drive-Mapping auf einen temporären Ordner des Hackers übertragen. Häufig genug werden auch noch vorhandene Backups auf dem System des Opfers gelöscht.
7. Ist die Anzahl der erbeuteten Daten aus Sicht des Angreifers ausreichend, wird der Anwender vom System ausgesperrt. Die Erpressungsnachricht mit einer Anleitung für die Übergabe des Lösegeldes (in Bitcoin) wird angezeigt. So wird dem Opfer ein Entschlüsselungscode ‚verkauft'.

Wie Sie Ihre Daten vor Ransomware schützen

„Es gibt keine generelle Methode oder Lösung, die Sie und Ihr Unternehmen komplett vor einem Ransomware-Angriff schützen wird. Sie sollten Möglichkeiten eines Angriffs in Betracht ziehen, einen Notfallplan ausgearbeitet haben und diesen regelmäßig überprüfen. Nur so können Sie einen ordnungsgemäßen Geschäftsbetrieb aufrecht erhalten" - FBI Cyper-Angriff, Abteilungsleiter James Trainor

Nutzen Sie grundlegende Präventivmaßnahmen!

Wenn keine Vorbereitungen getroffen wurden, bleibt häufig genug keine andere Wahl, als den Lösegeldforderungen eines Angreifers nachzugeben. Um dies zu vermeiden, ist Vorsorge die beste Verteidigung..

Grundlegende Präventivmaßnahmen, die Sie in Betracht ziehen sollten, um den Erfolg eines wahrscheinlichen Angriffs zu minimieren:

1. **Regelmäßige Backups:** Sichern Sie Ihre Daten regelmäßig. Überprüfen Sie ihre Vollständigkeit und sichern Sie auch Ihre Kopien. Lagern Sie Ihre Backups separat - also getrennt vom System und auch vom Netz. Überprüfen Sie routinemäßig Ihre Backup-Kopien. Denken Sie daran, dass Cyberkriminelle Sie nicht als Geisel nehmen können, wenn Sie eine Kopie Ihrer Daten jederzeit griffbereit haben.

2. **Patchen und updaten Sie alles:** Das Patchen und ein regelmäßiges Update Ihres Betriebssystems, der Antivirus-Software, des Browsers, von Adobe Flash und Java, der Remote-Access-Lösung sowie aller anderen verwendeten Software kann die Schwachstellen und somit die Möglichkeit zur Erpressung verhindern.

3. **Regelmäßige Computer Scans:** Stellen Sie sicher, dass Ihre Antivirus- und Antischadsoftware-Lösung automatisch und regelmäßig den gesamten Computer updatet und überprüft. Stellen Sie Ihre Sicherheitssoftware so ein, dass auch komprimierte und archivierte Ordner durchsucht werden, soweit möglich.

4. **Löschen Sie unsichere Remote-Services:** Ziehen Sie in Betracht, Remote-Access über RDP oder Terminal-Services zu deaktivieren. Port 3389 ist zu schließen. Dauerhafte IP-basierte Verbindungen (auch VPN) sind zu schließen. Aktivieren Sie VPN bei Bedarf. Stellen Sie sicher, dass Ihre Remote-Access-Lösung aktuellen Sicherheitsstandards entspricht. Remote-Access-Dienste sind beliebte Angriffspunkte. Cyberkriminelle suchen aktiv nach ungeschützten Ports von VNC, RDP und anderen gängigen Remote-Access-Lösungen.

5. **Keine Nutzung von erweiterten Rechten:**
Kein Nutzer sollte einen Administratorzugang haben, sofern er dies nicht unbedingt benötigt!.

6. **Erstellen Sie Passwort-Richtlinien:** Erstellen Sie generelle Passwort-Richtlinien für alle Nutzerkonten (mit Remote-Access). Verwenden Sie individuelle und „starke" Passwörter für die verschiedenen Accounts.

7. **Nutzen Sie Whitelisting von Anwendungen:** Erlauben Sie den Systemen, nur die Programme auszuführen, die Ihnen bekannt sind und die auch Ihren Sicherheitsrichtlinien entsprechen.

8. **Deaktivieren Sie Macros und Scripts:** Deaktivieren Sie Windows Script Host, Windows Powershell, Macros und ActiveX. Blockieren Sie das Ausführen von externen Inhalten. Das ist eine verlässliche Methode, um schädlichen Code von Ihren Geräten fern zu halten.

9. **Verwenden Sie Softwareeinschränkungen:** Verhindern Sie, dass Programme aus typischen Ransomware-Ordnern, wie z.B. temporäre Download-Ordner der bekannten Browser oder auch Ordner von Entpackprogrammen, ausgeführt werden können.

10. **Deaktivieren Sie Autoplay:** Stellen Sie sicher, dass gefährliche Programme nicht automatisch von einem externen Medium, wie einem USB Stick oder anderen Geräten, starten können.

11. **Schulen Sie Ihr Personal:** Entwickeln Sie ein ausgeprägtes Sicherheitsbewusstsein bei Ihren Mitarbeitern. Regelmäßiges Training der Mitarbeiter fördert den Umgang und die Vorsicht mit kritischen E-Mails, Anhängen und Downloads.

12. **Wählen Sie Ihre Lösungsanbieter gut aus:** Wählen Sie gezielt bewährte Anbieter und Lösungen für Ihre vertraulichen Daten aus. Open-Source-Software und Freeware können zwar sehr hilfreich sein - bei Fragen der Sicherheit und dem Schutz Ihrer vertraulichen Daten und/oder Infrastruktur ist eine Investition in eine erprobte Technologie, die anhaltenden Support und Updates bietet, allerdings definitiv die bessere Lösung, um Risiken zu verringern.

Bedenken Sie, dass eine Organisation nur dann gut gegen Bedrohungen geschützt ist, wenn Sicherheitsmaßnahmen sowie Vorsorge- und Notfallpläne umgesetzt und regelmäßig aktualisiert werden.

„Unternehmen sollten niemals schwache oder Standard-Passwörter nutzen und sich stattdessen auf eine Passwort-Richtlinie stützen, die vom Sicherheitsbeauftragten erstellt wurde und vom IT-Personal umgesetzt wird." - Dominik Samociuk, IT Sicherheits-Ing. bei Future Processing (Millman, 2015)

Verwenden Sie sichere Remote-Control- und Remote-Access-Lösungen.

„Eine neuer Trend im Bereich Ransomware wurde festgestellt. Die Verbreitung erfolgt über Remote-Desktop- oder Terminal-Service-Hacks." - SC Magazine (Millman, 2015)

Mit diesem neuen Trend nutzen Cyberkriminelle Schwachstellen der Remote-Access-Tools aus, um in Kassensysteme, Zahlungssysteme, Rechenzentren und selbst in Geldautomaten einzudringen.

„Unternehmen sollen sich auch den Wechsel zu anderer Remote-Desktop-Software überlegen, wenn sie sich mit der Out-of-the-box Funktionalität von Windows unwohl fühlen. Wie bei den meisten Dingen ist - auch bei Ransomware - ein guter Notfallplan die sicherste Lösung. Kein Abwehrsystem ist narrensicher"

- Chris Boyd, Malware Technologieanalyst bei Malwarebytes (Millman, 2015)

No safeguard is completely foolproof on its own, but the right combination of preventive actions will significantly lower your risk of a ransomware attack.

Bei der Auswahl der richtigen Remote-Control- und Remote-Access-Lösung sollten Sie auf folgende grundlegenden Sicherheitsfunktionen achten, nur so erhalten Sie einen vernünftigen Schutz gegen Ransomware:

1. **Gesicherte Übertragung:** Vertrauliche Informationen sollten während einer Übertragung verschlüsselt sein, um unautorisierte Einsicht zu verhindern. Wählen Sie einen Anbieter, der mit 256-bit-Verschlüsselung und dynamischen Schlüsselaustausch arbeitet, um die Daten Ihres Unternehmens und Ihrer Kunden zu schützen.

2. **Kontrollieren Sie den Nutzer-Zugriff::** Nutzen Sie eine Ende-zu-Ende-Authentifizierung. Der Nutzer muss sich an jedem Standort und bei jeder Verbindung authentifizieren. Nutzen Sie darum nur Lösungen, die eine Multifaktor-Authentifikation wie auch geschlossene Benutzergruppen bereitstellen.

3. **Verwalten Sie Zugriffsrechte:** Der Zugriff auf vertrauliche Daten sollte durch das Unternehmen eingeschränkt sein. Nur derjenige, der gewisse Daten auch tatsächlich benötigt, darf Zugriff auf diese Daten haben. Stellen Sie sicher, dass verschiedene Nutzer auch verschiedene Zugangsprofile bekommen. Ihre Remote-Access Lösung benötigt dafür ein fein abstufbares Nutzerzugriffs-Management..

4. **Monitoren Sie alle Aktivitäten:** Es muss nachvollziehbar sein, wer wann was und wo im Rahmen einer Remote Session getan hat. Nutzen Sie im Bedarf eine ausgelagerte Verfilmung und Archivierung aller Sessions, um Revisionssicherheit zu erreichen.

Nächste Schritte

Überprüfen Sie die in Ihrem Unternehmen eingesetzten Remote-Access Lösungen. Ihre Lösung sollte die Standards für PCI übertreffen. Durch den Einsatz von zusätzlichen Sicherheitsfunktionen, wie der Multi-Faktor Authentisierung, dem Logging der Aktivitäten von Remote Sessions und fest definierten Zugriffsrechten, kann man die Vorteile eines Remote-Access-Zugangs weiterhin nutzen. Gleichzeitig wird durch diese Sicherheitsfunktionen das Risiko eines Ransomware Angriffs auf Ihr Unternehmen oder Ihre Kunden weitestmöglich reduziert. Nehmen Sie Kontakt zu uns auf, wenn Sie erfahren möchten, wie Sie Ihr Remote-Access-System noch sicherer machen können.

Geben Sie sich nicht mit „ein bisschen Sicherheit“ zufrieden!

Wenn es um Remote-Desktop-Access und Remote-Support geht, ist Netop Remote Control (NRC) eindeutig und bekannter Weise einer der Marktführer in diesem Segment. NRC bietet Ihnen die sofortige Kontrolle über Keyboard, Video und Maus auf fast jedem Gerät oder OS. Eine marktführende Verschlüsselung, die Multi-Faktor Authentifizierung und das detaillierte Logging geben Ihnen ein Maß an Sicherheit, wie Sie es bei keiner anderen Remote Access Lösung erhalten werden.

Wir glauben, dass Sicherheit und Effizienz sich keinesfalls ausschließen müssen. Für den IT-Support und den Help-Desk ist Netop Remote Control die einzige Lösung, die allen gängigen Sicherheitsstandards und -vorgaben entspricht. Vereinfachen Sie Ihre Wartungsarbeiten bei gleichzeitiger Eingrenzung von Schwachstellen in Ihrem Netzwerk. Bündeln Sie Ihre Remote-Access-Dienste in einer einfach zu bedienenden Oberfläche.

Die schnelle Lösung von Alltagsproblemen bedeutet einen besseren Arbeitsablauf und reduziert die Betriebskosten. Unterstützen Sie Ihre Kunden aus der Ferne innerhalb und außerhalb Ihres LAN-Bereichs. Aus der Cloud oder auch klassisch als lokale Host-Lösung.

Mit Netop erstellen Sie sichere On-Demand Tunnel zu beliebigen Systemen, um aus der Ferne Programme und Anwendungen zu steuern. Sie erhalten Zugang zu Daten, die Ihr Unternehmen braucht. Ihre Kunden erhalten im Gegenzug einen besseren Service. Durch Vergabe von sehr granularen Rechten können Sie externen Dienstleistern den sicheren Zugang zu explizit ausgewählten Systemen gewähren.

Lesen Sie hier mehr über Netop Remote Control’s Sicherheitsstrategien.

Zitierte Werke

Incidents of Ransomware on the Rise (2016, April 29).
https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

lindagerrits. (2016, May 2). Ransomware deployments after brute force RDP attack [Blog Post].
https://blog.fox-it.com/2016/05/02/ransomware-deployments-after-brute-force-rdp-attack

Millman, R. (2015, October 21). Ransomware using Remote Desktop to spread itself.
http://www.scmagazineuk.com/ransomware-using-remote-desktop-to-spread-itself/article/448377/

Quellenverzeichnis

http://www.scmagazineuk.com/ransomware-using-remote-desktop-to-spread-itself/article/448377/

https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962

http://support.eset.com/kb3433/?locale=en_US

https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

http://idt911.com/sites/default/files/uploads/2014/03/030714_Retailer_300ppi-01.png

https://www.markmonitor.com/solutions/industry_solutions-financial-services.php

https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked