RANSOMWARE – Eine Gefahr für Unternehmen

ENJOY SAFER TECHNOLOGY™

INHALT

Author: Stephen Cobb
Danksagung: Dieses Whitepaper hätte nicht geschrieben werden können ohne die Hilfe meiner Kollegen bei ESET, James Rodewald, Ben Reed, Fer O'Neil, und David Harley, und ohne mein motiviertes Team Aryeh Goretsky, Bruce P Burrell, Cameron Camp, und Lysa Myers.

Ziele und Zusammenfassung

Dieses Whitepaper soll erläutern, warum Ransomware noch immer eine nicht zu unterschätzende Gefahr für Unternehmen darstellt – und was getan werden kann, um sich vor ihr zu schützen. Damit soll vor allem CEOs, CIOs, CISOs und Risikomanagern ein Werkzeug an die Hand gegeben werden, um aktuelle Entwicklungen genau zu verstehen, nachzuvollziehen, und zu erfahren, worauf beim Ransomware-Schutz zu achten ist.

Wir beschäftigen uns dabei vor allem mit drei Einfallstoren für Ransomware: Remote-Verbindungen, E-Mails sowie die (Software-) Lieferkette. Anhang B gibt zusätzlich Einblick in technische Details typischer Ransomware-Angriffe und möglicher Abwehrmechanismen.

Ransomware

Bei Ransomware handelt es sich um eine spezielle Art von Malware. Während Malware als Sammelbegriff für alle Arten von Schädlingen, wie Viren, Würmern oder Trojanern gilt, bezeichnet Ransomware Schadcode zum Erpressen von Lösegeld. Diese Erpressersoftware wird dabei in drei Kategorien unterteilt:

- LockScreens, die den Bildschirmzugang des Geräts sperren,
- Krypto-Ransomware, die Daten verschlüsselt und
- Schadsoftware, die Daten löscht (Wiperware) oder die Geräte anderweitig als sogenannte „Brickware" unbrauchbar macht (zum Beispiel durch die Veränderung des Master Boot Record -Codes).

Bei letzterer können die Daten nicht entschlüsselt oder anderweitig wiederhergestellt werden. Der bekannte Schädling NotPetya/Diskcoder.C ist solch eine Ransomware als Kombination aus Wiper- und Brickware.

Ransomware-Angriffe sollten nicht mit DoS (Denial of Service)-Attacken verwechselt werden. Hierbei wird der Zugriff auf Unternehmensdaten zwar auch blockiert, dies geschieht jedoch durch die Überlastung der Server durch zu viele Anfragen in zu kurzer Zeit. Es werden keine Daten manipuliert. Angreifer wollen hiermit *Lösegelder* von Webseitenbetreibern erpressen und drohen, die Seite kurzfristig unerreichbar zu machen. Das ist vor allem für Händler dramatisch: Dieses Vorgehen können einen bedeutenden finanziellen Verlust bedeuten, selbst wenn ein Ausfall nur für eine begrenzte Zeit eintritt. DoS-Attacken sind auch bei *sogenanntem Hacktivismus* und *Angriffen auf Konkurrenten* beliebt.

Echte Ransomware hingegen manipuliert Dateien so, dass ihr eigentlicher Inhalt wiederhergestellt werden kann und dies im Allgemeinen so lange, bis eine Lösegeldforderung beglichen wurde. Die Idee, Daten und Rechner als „Geiseln" zu nehmen ist dabei keineswegs neu. Donn Parker berichtete bereits 1971 in seinem wegweisenden „Crime by Computer" von einem Fall. *Dr. Popp's AIDS-Trojaner* von 1989 gilt dann als die erste Ransomware, die die Daten von Opfern verschlüsselte und sie erst gegen Zahlung eines Lösegeldes wieder entschlüsselte.

Glücklicherweise fanden diese beiden Fälle zunächst keine Nachahmer. Erst viele Jahrzehnte später gewann Ransomware an Bedeutung. Vor allem in den letzten fünf Jahren mehren sich Berichte über Ransomware-Angriffe auf größere Ziele. Besonders aufsehenerregend war dabei WannaCryptor im Jahr 2017. Wie interessant das Thema scheinbar ist, zeigt sich auch daran, dass einer der 5 meistgelesenen Artikel auf der internationalen Version von WeLiveSecurity der Artikel *„11 things you can do to protect against ransomware, including Cryptolocker"* von ESET-Expertin Lysa Myers aus dem Jahr 2013 ist. Weitere Zahlen beziffern das Ausmaß der Entwicklung:

- Weltweit stieg die Anzahl an Ransomware-Attacken 2017 im Vergleich zu 2016 um 350 Prozent (Dimension Data, 2018)

- 48 Prozent aller IT-Consultants berichten von Supportanfragen zum Thema Ransomware in 22 verschiedenen Branchen (Intermedia 2017).
- 25 Prozent aller Versicherungsfälle 2017 im IT-Bereich hatten mit Ransomware zu tun (AIG, 2018).
- Der durch WannaCryptor verursachte Schaden wird auf bis zu 4 Milliarden US-Dollar beziffert (Cyence, 2017).
- 72 Prozent aller von Ransomware-Angriffen betroffenen Unternehmen konnten mindestens für zwei Tage nicht auf ihre Daten zugreifen. Bei 32 Prozent waren es sogar fünf oder mehr Tage (Intermedia, 2017).

So beeindruckend diese Zahlen auch sind: Sie helfen scheinbar nicht, Unternehmen auf Ransomware aufmerksam zu machen und Angriffe zu verhindern. Dieses Whitepaper soll hier Abhilfe schaffen.

Ransomware ist und bleibt gefährlich

Falls Ihr Unternehmen erst kürzlich Opfer einer Ransomware-Attacke war, mag Ihnen dieses Whitepaper und sein Ziel, auf die Gefahren dieser Schadsoftware-Familie aufmerksam zu machen, wenig interessant erscheinen. Sind Sie jedoch bisher von Ransomware verschont geblieben, denken Sie vermutlich – auch durch entsprechende Schlagzeilen – dass Ransomware ein alter Hut sei und Unternehmen wie Privatleute sich viel mehr vor dem Missbrauch ihrer Rechner durch Fremde für das Schürfen von Bitcoins, Ethereum oder anderen Krypto-Währungen in Acht nehmen sollten. Sicherlich ist Kryptomining eine ernsthafte Bedrohung, die in den kommenden Jahren voraussichtlich noch mehr an Bedeutung gewinnen wird, andererseits durch IT-Security-Lösungen relativ einfach zu erkennen ist. Die Bedrohungslage im IT-Sektor ist jedoch hoch komplex und ständigen Wandlungen unterworfen. Anzunehmen, dass eine Gefahr in dem Maße abnimmt, wie andere zunehmen, ist kurzsichtig und kann höchst gefährliche Folgen haben.

Tatsächlich ist die Gefahr durch Ransomware aktuell größer denn je. Vor allem in den letzten beiden Jahren haben Cyberkriminelle ihre Methoden perfektioniert, Ransomware auf Systeme aufzuspielen. Im Vergleich zu früher, als Kriminelle viele Nutzer um verhältnismäßig geringe Summen erpressen wollten, gehen sie nun wesentlich gezielter vor. Sie konzentrieren sich auf einen eher kleinen Kreis von besonders attraktiven Opfern, deren Daten einen besonders hohen Wert haben und von denen sich deshalb große Summen erpressen lassen.

Natürlich ist auch der Verlust von Familienfotos und anderen wertvollen privaten Daten sehr ärgerlich und sollte möglichst vermieden werden. Erfolgreiche Ransomware-Angriffe auf Unternehmen und deren Daten ziehen aber oft ungleich größere wirtschaftliche und gesellschaftliche Schäden nach sich. Im Fall der Stadtverwaltung von Atlanta, der Hauptstadt des US-Bundesstaates Georgia, weigerte man sich zwar richtigerweise, die 50.000 Dollar Lösegeld zu bezahlen, hat nun aber mit einem umso größeren finanziellen Schaden zu rechnen. (Schätzungen gehen aktuell von *bis zu 17 Millionen Dollar* aus.) Fünf Abteilungen der Stadtverwaltung mussten bis zu eine Woche ohne arbeitsfähige Rechner auskommen. Die Wasserwirtschaft, die Personalabteilung, die Gefängnisverwaltung sowie die Abteilungen für Parkanlagen und Stadtplanung waren durch den Angriff betroffen und konnten unter anderem keine Zahlungen, z.B. für Wasserrechnungen oder Strafzettel, annehmen. Auch das WLAN auf dem internationalen Flughafen Hartsfield-Jackson Atlanta war für eine ganze Woche nicht erreichbar.

Nun sind natürlich bei Weitem nicht nur Organisationen in öffentlicher Hand von Ransomware-Attacken betroffen. Diese sind aber meist dazu verpflichtet, Datenlecks und ähnliche Vorfälle publik zu machen. Insbesondere im Gesundheitswesen erfordert der *Schutz von Patientendaten* die Offenlegung aller datenschutzrelevanten Vorfälle. Wir wissen deshalb von mehreren Angriffen auf Regierungsorganisationen und medizinische Versorgungseinrichtungen im Jahr 2018 durch eine Ransomware-Familie namens SamSam. (ESET bezeichnet diese als *MSIL/Filecoder.Samas.*) SamSam ist bereits seit 2016 bekannt dafür, auf verschiedensten Wegen in Systeme einzudringen. Anfang 2018 wurde jedoch bekannt, dass die Schadsoftware vermutlich über „Brute-Force-Attacken auf RDP-Endpoints" in Netzwerke eindringt (*US Department of Health and Human Services*).

Doch auch Unternehmen des privaten Sektors sind und bleiben beliebte Angriffsziele. Allerdings ist hier davon auszugehen, dass sie versuchen, erfolgreiche Ransomware-Attacken auf ihre IT-Infrastruktur geheim zu halten, um negative PR zu vermeiden. Entsprechend können wir das Ausmaß der Gefahr auf privatwirtschaftliche Betriebe nur schwer anhand von Medienberichten beziffern. Wir wissen aber aus Gesprächen mit Managed Service Providern und Anbietern von Security-Software, dass Ransomware weiterhin eine große und vor allem potentiell kostspielige Gefahr für alle Branchen darstellt.

RDP (Remote Desktop Protocol)

Ein RDP-Endpoint, z.B. ein Datenbank-Server, dient dazu, RDP (Remote Desktop Protocol)-Software auszuführen, damit das Gerät von außen, also zum Beispiel über das Internet, erreicht werden kann. Ein potentieller Angreifer kann in theoretisch unbegrenzt vielen Anläufen in sehr kurzen Abständen versuchen, die Zugangsdaten eines Servers zu erraten. Wird die Anzahl der Versuche nicht limitiert, ist es dem Angreifer so ein Leichtes, Zugriff auf den Server zu bekommen.

Dies erfordert zwar mehr Aufwand als Ransomware, die einfach per E-Mail versendet wird, bietet aber auch viele Vorteile für den Angreifer. Schutzmechanismen von Endpoints lassen sich einfach umgehen und schon innerhalb kürzester Zeit können viele Systeme innerhalb eines Netzwerks infiziert werden. Nehmen wir zum Beispiel den Angriff via RDP auf LabCorp, einen der größten Medizininstrumente-Hersteller in den USA im Juli 2018: Obwohl das Unternehmen in der Lage war, den Angriff innerhalb von 50 Minuten einzudämmen, waren bereits 7000 Rechner und 350 Server infiziert (CSO).

RDP basierte Angriffe werden oftmals selbst von hoch entwickelter Sicherheitssoftware nicht erkannt. Entsprechend gering ist oftmals das Bewusstsein, wie gefährlich diese Attacken tatsächlich sind. So kann beispielsweise jedes Unternehmen mit einem halbwegs ausgereiften Security-System per E-Mail verschickte Ransomware ohne Probleme erkennen und blockieren. Entsprechende Vorfälle werden automatisch gemeldet und dokumentiert, sodass Security-Anbieter umfangreiche anonymisierte Statistiken erstellen können und die aktuelle Ransomware-Variante schnell an Einfluss verliert. Ähnliches gilt für Webseiten, die Ransomware verteilen. Hat der Angreifer jedoch Admin-Rechte für einen Server, kann er die Sicherheitssoftware schlicht deaktivieren, bevor er die Ransomware auf einen Endpoint aufspielt. Die jeweilige Ransomware-Variante taucht so in keiner Statistik auf.

Bei RDP handelt es sich tatsächlich um ein sehr nützliches Protokoll, ermöglicht es doch den Zugriff auf Unternehmensrechner von außen. Das ist zum Beispiel äußerst praktisch, um zentrale Datenbanken zu pflegen oder gemeinsam genutzte Software zu verwalten.

Mitarbeiter verbinden sich per RDP mit dem Server, z.B. mit ihren Laptops. Wird die Netzwerkadresse des Remote-Systems eingegeben, verbindet sich die Client-Software mit dem entsprechenden Port auf dem Server. (Der Standard-Port für RDP ist 3389. Dieser kann und sollte allerdings umgehend geändert werden.) Die Software auf dem Server öffnet nun ein Login-Fenster, welches zur Eingabe von Benutzername und Passwort auffordert. Abbildung 1 zeigt ein solches Fenster in einer Windows-Umgebung.

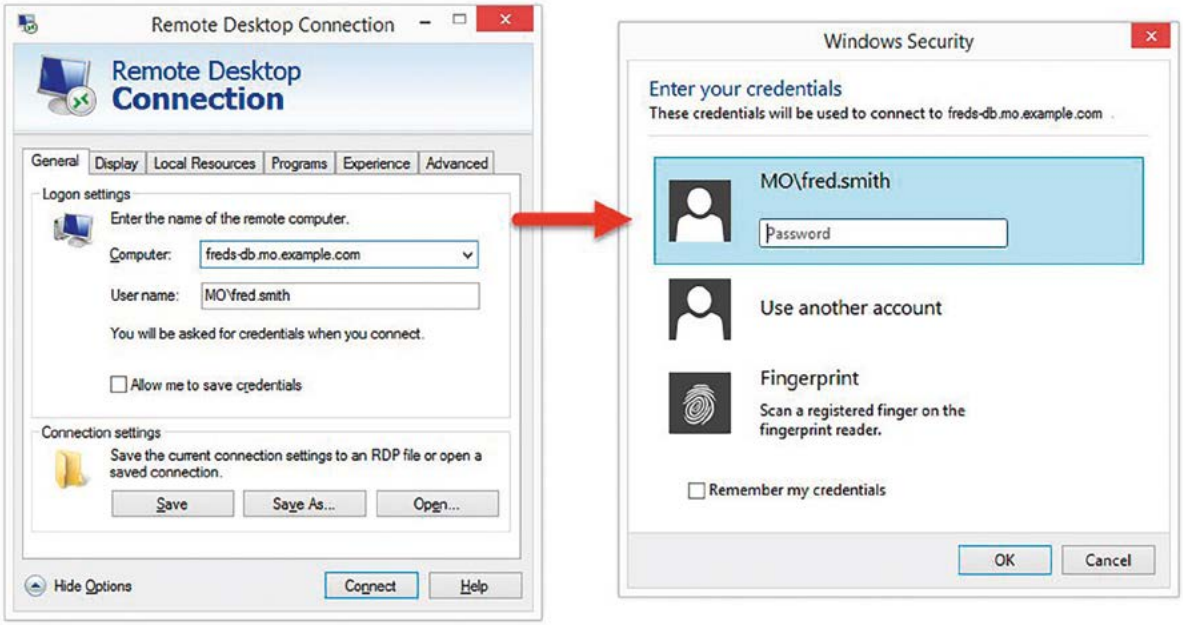

Abbildung 1

Wie mein Kollege bei ESET, James Rodewald, erläutert, kommt RDP für zwei typische Unternehmensanwendungen zum Einsatz: Zum einen dient es dazu, Programme auf einem Server zu verwalten, z.B. eine Webseite oder eine Backend-Datenbank. Hierzu gibt der System-Administrator anderen Admins Zugriff auf Port 3389. Außerdem wird RDP verwendet, um Nutzern ohne Admin-Rechte die Arbeit auf einem gemeinsamen System zu ermöglichen. Dies kann im Unternehmensnetzwerk oder von außerhalb über das Internet geschehen. In letztgenanntem Fall ist Port 3389 für die Außenwelt zugänglich. Kriminelle können relativ einfach Zugriff auf RDP-Server erlangen:

- Unzureichend geschützte Server sind leicht zu finden – insbesondere dann, wenn die Werkseinstellungen des Servers nicht neu oder schlecht konfiguriert wurden.
- Sind entsprechend verwundbare Server gefunden, nutzen die Angreifer Methoden zur Erlangung von Admin-Rechten, wie sie sich ganz einfach im Internet finden lassen.

RDP-Server lassen sich leicht mit speziellen Suchmaschinen wie z.B. Shodan ausfindig machen. Diese durchsuchen laufend das Internet nach verbundenen Geräten und sammeln Informationen über sie. Eine Suche per Shodan.io am 13. Dezember 2018 ergab, dass mehr als drei Millionen Systeme weltweit *Port 3389* verwenden. (Für die vollständige Ansicht gefilterter Suchanfragen ist eine Registrierung notwendig). Wie in Abbildung 2 zu sehen ist, stehen mehr als 100.000 Systeme in Deutschland.

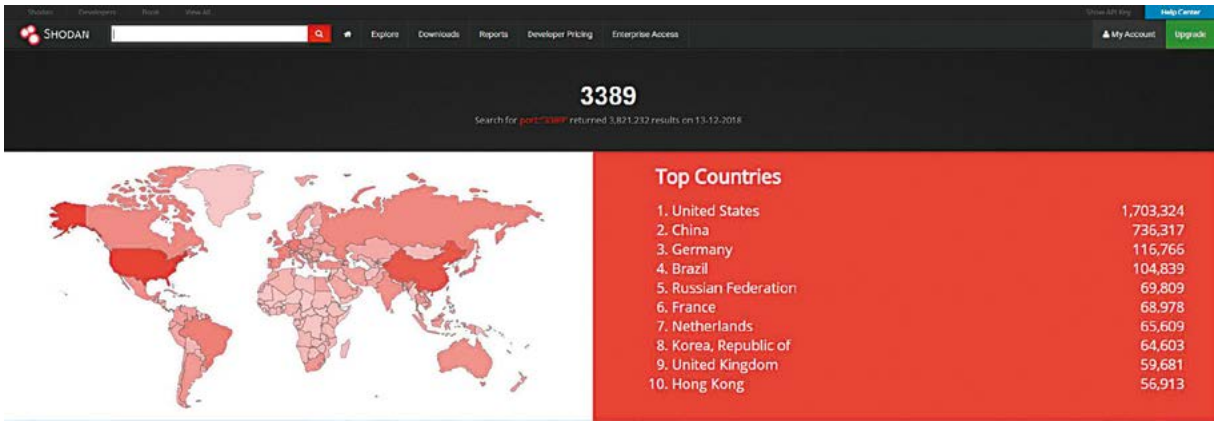

Abbildung 2

Eine weitere Suchanfrage ergab, dass mehr als 2 Millionen Rechner *explizit RDP* verwenden und so besonders attraktive Ziele darstellen. Zwar werden im Allgemeinen Zugangsdaten für den Login auf einen RDP-Server benötigt, diese sind jedoch überraschend einfach zu erraten, insbesondere, wenn die Angreifer Brute Force verwenden, also mehrfach und in kurzen Zeitabständen versuchen, sich mit plausiblen Zugangsdaten auf den Server einzuwählen.

Noch einfacher ist es für Angreifer, die ausreichend finanzielle Ressourcen besitzen, um Zugangsdaten einfach im Dark Web zu kaufen. Über die Webseite xDedic beispielsweise werden solche und ähnliche Daten angeboten. Damit lassen sich Angriffe bereits in einem frühen Stadium fokussieren. So kann zum Beispiel nach Standort, Betriebssystem, CPU, RAM, Geschwindigkeit der Internetverbindung, installierten Anwendungen, Blacklist-Status, aktuell installierter Antiviren-Software und vielem mehr gefiltert werden. Weitere Informationen hierzu finden sich in Anhang A.

Der Kauf von Login-Daten für Server ist natürlich nicht nur für geplante Ransomware-Angriffe interessant. Tatsächlich listet xDedic selbst 12 verschiedene Anwendungsmöglichkeiten für gehackte Server auf, darunter Spamversand und Malware-Hosting, Passwortdiebstahl, Kryptomining und weitere Anwendungen, bei denen der Verantwortliche anonym bleiben möchte, z.B. Käufe illegaler Güter und Geldwäsche. Die Seite

bietet auch bereits vorgefertigte Tools, mit denen sich fremde Server für illegale Aktivitäten missbrauchen lassen.

Serverparasiten

Für Kriminelle kann ein gekaperter Server noch wesentlich mehr Nutzen bringen als ein bloßes Lösegeld für verschlüsselte Daten. Er kann zum Beispiel Ausgangspunkt einer großflächigeren Attacke sein, mit denen der Angreifer Zugriff auf ein ganzes Netzwerk von Geräten erlangt. Hier kann er wiederum Daten auf noch wesentlich mehr Rechnern verschlüsseln. Die Methoden, mit denen solche Angriffe durchgeführt werden, sind dabei weder sonderlich komplex noch schwer in Erfahrung zu bringen.

Hat er einmal Zugriff auf einen Server erhalten, versucht der Angreifer im Allgemeinen, so viel wie möglich darüber herauszufinden, wie dieser sich für seine Zwecke nutzen lässt. Hat er den Zugriff nicht sowieso schon über die Adminrechte erlangt, kann er sich verschiedener Techniken bedienen, um diese nachträglich zu erlangen. Ist eine Endpoint Security Lösung auf dem System installiert, und kann diese mit Adminrechten abgeschaltet werden, ist sehr wahrscheinlich, dass der Angreifer dies möglichst schnell tun wird. So ist es für ihn ein Leichtes, zusätzliche Software herunterzuladen, mit denen er das Potential, was ihm nun zur Verfügung steht, umfassend nutzen kann.

(Anm.: Wenn wir vom „Angreifer" reden, meinen wir nicht unbedingt eine Person, die vor einem Rechner sitzt und die Aktivitäten ausführt. Große Teile der Angriffe werden automatisiert durch Software durchgeführt.)

Um nicht entdeckt zu werden, versuchen die Angreifer, möglichst wenig Schadcode auf die infizierten Systeme aufzubringen. Stattdessen missbrauchen sie oftmals bekannte legitime Software für ihre Zwecke. NotPetya beispielsweise bediente sich der beiden Tools PsExec und Windows Management Instrumentation Command-Line (WMIC) um sich durch das infizierte Netzwerk zu bewegen. Da es sich hierbei um viel verwendete, legitime Programme handelt, ist ein Missbrauch nur schwer zu identifizieren, wenn nicht sogar unmöglich. (Im Abschnitt zu EDR-Tools werden wir auf dieses Thema noch genauer eingehen.)

Eine weitere Strategie von Ransomware, sich in einem Netzwerk zu verbreiten, besteht darin, sich in einem verhältnismäßig leicht zu kompromittierenden System einzunisten und von dort aus erreichbare Systeme zu infizieren. Bei einem Angriff auf ein Krankenhaus im US-amerikanischen Greenfield, Indiana, beispielsweise verwendeten die Angreifer „gestohlene Zugangsdaten, um einen Backup-Server zu infiltrieren, der mehrere Kilometer vom eigentlich Hauptcampus entfernt steht. Von dort aus wurde über das Netzwerk der Hauptrechner auf dem Campus erreicht und SamSam installiert," (*HHS Report*).

Nicht zuletzt nutzen Angreifer natürlich auch bisher ungepatchte Schwachstellen in legitimer Software. So konnte sich z.B. durch den *EternalBlue Exploit*, welcher eine Schwachstelle in Microsofts Server Message Block (SMB)-Protokoll ausnutzt, WannaCry ungehindert verbreiten (siehe *Microsoft Security-Bulletin MS17-010*). Lediglich Systeme, deren Endpoint-Schutz *EternalBlue* blockierten, waren davor sicher.

Alle oben genannten Angriffe sind nachhaltig und großflächig angelegt. Natürlich haben Angreifer aber auch immer die Möglichkeit, mit relativ geringem Aufwand schnelles Geld zu machen, indem sie einfach einen Server kapern, Daten verschlüsseln und Lösegeld fordern.

Abwehr

Glücklicherweise ist es mit nur sehr geringem Aufwand möglich, RDP-Server gegenüber unerlaubtem Zugriff zu schützen. Der folgende Abschnitt soll erläutern, welche Maßnahmen sinnvoll sind. Technologische Details zum Vorgehen finden sich in Anhang B.

Bestandteil vieler Sicherheitspolicys in Unternehmen ist es, Zugriffe auf das Netzwerk von außen genauestens zu regeln. So gibt es vermutlich auch in Ihrem Unternehmen die Vorgabe, dass alle RDP-Zugriffe nur per VPN möglich sind, dass sie durch Zwei-Faktor-Authentifizierung abgesichert werden müssen, nur von bestimmten Rollen und nur auf besonders geschützten Systemen durchgeführt werden dürfen, laufend überwacht und durch eine Firewall geschützt werden müssen. Regelmäßige Backups sind ebenfalls oft verpflichtend.

Diese Regeln, seien sie geplant oder bereits implementiert, sind allerdings keine Garantie, dass Ihr Remote-Zugang nicht doch gehackt werden kann. Vor allem muss darauf geachtet werden, dass jeder einzelne Mitarbeiter die Vorgaben verinnerlicht hat und strikt einhält. Unabhängig von allen Sicherheitsvorkehrungen müssen zudem Maßnahmen geplant werden, die im Falle eines Vorfalls helfen, möglichst schnell zum Status Quo zurückzukehren.

Grundvoraussetzung für eine funktionierende Absicherung Ihrer IT-Infrastruktur ist der vollständige und laufend aktuelle Überblick über alle mit dem Internet verbundenen Systeme im Unternehmen. Es mag komisch klingen, aber wenn Sie nicht wissen, dass sich ein Gerät in Ihrem Netzwerk befindet, können Sie es auch nicht schützen. Dieser Fall ist übrigens laut unseren Recherchen gar nicht so selten: Vielfach wussten Sicherheitsverantwortliche vor einem Angriff über bestimmte Geräte nicht, dass diese überhaupt Teil des Unternehmensnetzwerks sind.

Damit Ihnen das nicht passiert, können Sie verschiedene Vorkehrungen treffen. Zentral ist, dass es z.B. für externe Dienstleister oder Mitarbeiter nicht möglich sein sollte, einen physischen oder virtuellen Server mit dem Unternehmensnetzwerk oder dem Internet zu verbinden – es sei denn, dieser ist vernünftig konfiguriert und zwar bevor der Server online geht.

Case Study: Die Attacke auf CDOT

Einem *Bericht aus dem Juli 2018* zufolge begann die Attacke auf die Verkehrsbehörde von Colorado (Colorado Department of Transportation, CDOT) im Februar 2018 mit einem virtuellen Server, der bereits zwei Tage nach seinem Aufsetzen per Internetverbindung gekapert werden konnte. Die Angreifer „benötigten 40.000 Versuche, um das Passwort für den Admin-Account zu erraten."

Haben Sie den Überblick über alle mit dem Internet verbundenen Geräte in Ihrem Netzwerk erhalten, muss in Erfahrung gebracht werden, welche per Remote Access erreichbar sind – und, ob dies überhaupt nötig ist. Ist der Zugang tatsächlich notwendig, sollte ermittelt werden, ob das Gerät nicht alternativ im internen Netzwerk platziert oder per VPN erreicht werden kann.

Muss ein Gerät per öffentlichem Internetzugang via RDP zugänglich sein und kann kein VPN verwendet werden, sollte zumindest eine Zwei-Faktor-Authentifizierung eingerichtet werden, sodass Accounts nicht so leicht gehackt werden können. Allerdings sollte diese auf *keinen Fall SMS-basiert* sein. *SMS basierte Authentifizierung* lässt sich auf verschiedenste Arten missbrauchen, wie vor allem durch Angriffe auf *europäische Banken*, die dieses System seit langem nutzen, gezeigt wurde.

Kann – aus welchen Gründen auch immer – keine 2FA implementiert werden, sollte zumindest vermieden werden, dass Angreifer durch wiederholtes Raten Zugangsdaten in Erfahrung bringen können. Dies lässt sich zum Beispiel bewerkstelligen, indem eine Höchstzahl erfolgloser Versuche zu einer Sperrung für eine gewisse Zeit führt. Abbildung 3 zeigt, wie so etwas in der Praxis auf Windows aussehen könnte.

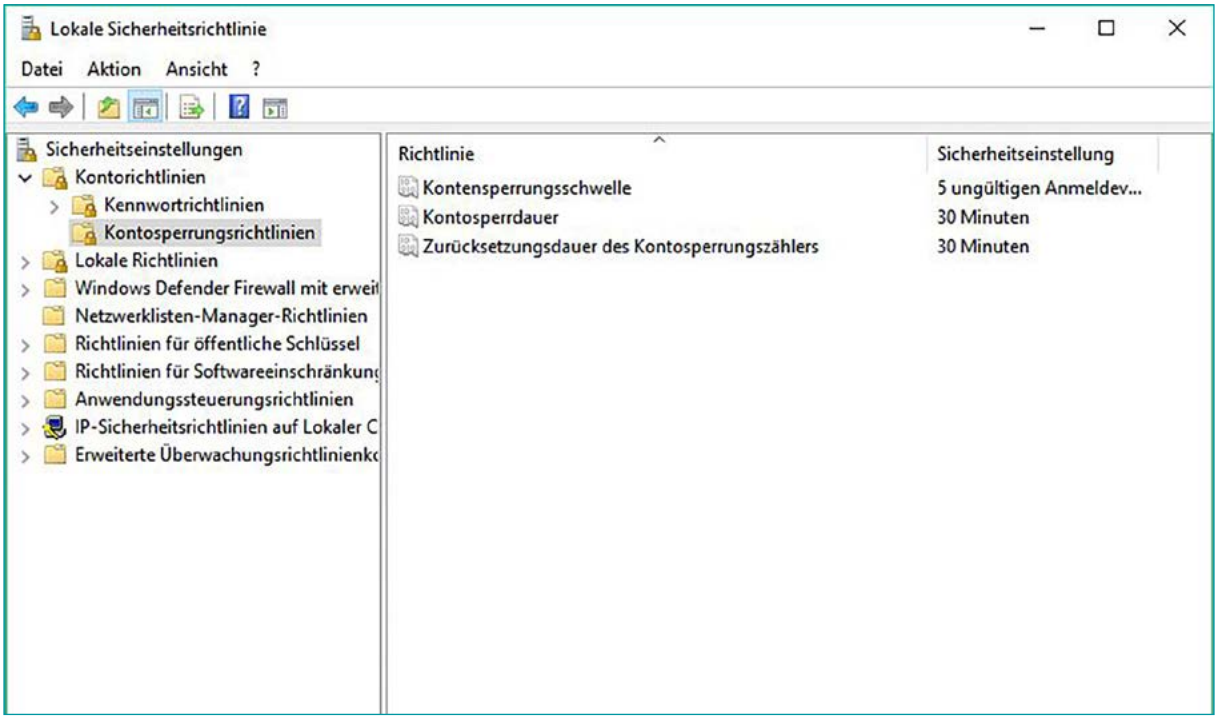

Abbildung 3

Eine weitere, einfach umzusetzende Maßnahme ist, den lauschenden Port des Servers von 3389 auf einen anderen Port umzustellen. So ist es für Angreifer schwerer, den Server als potentiell angreifbares Ziel zu identifizieren. Dies lässt sich unkompliziert über die Systemeinstellungen bewerkstelligen. Allerdings müssen entsprechend auch die Firewall-Einstellungen geändert werden, um sie den Änderungen anzupassen. Zu beachten ist auch, dass diese „Tarnung" nur geringen Schutz bietet und nicht die einzige Maßnahme zur Absicherung sein sollte. (Siehe auch Anhang B.)

Alle von außen erreichbaren Systeme sollten zudem regelmäßig gepatcht und abgesichert werden. WannaCry zum Beispiel konnte sich deshalb so schnell verbreiten, weil so viele ungepatchte Instanzen von SMB existierten. Es sollte auch dafür gesorgt werden, dass alle nicht benötigten Dienste und Komponenten entfernt oder deaktiviert werden und dass die weiteren Konfigurationen auf maximale Sicherheit ausgerichtet sind. Auf Windows-Systemen z.B. lassen sich Einschränkungen für Software setzen, sodass Dateien nicht aus den Ordnern AppData und LocalAppData ausgeführt werden – ein ganz typisches Verhalten von Malware.

Nicht zuletzt sorgt ein umfassendes und erprobtes Backup- und Wiederherstellungssystem für Sicherheit gegenüber Ransomware. Da es sich hierbei um einen zentralen Aspekt bei der Schadenabwehr handelt, werden wir später noch einmal genauer darauf eingehen.

Ransomware in E-Mails und andere Angriffsvektoren

Auch wenn es durch Trends in der Berichterstattung manchmal so wirken mag: Wie schon erwähnt, treten IT-Bedrohungen nicht nacheinander auf. Nur weil aktuell Ransomware-Angriffe vor allem über von außen zugängliche Server durchgeführt werden, heißt das nicht, dass andere Einfallstore ignoriert werden sollten. Noch immer werden E-Mails verschickt (und ihre Anhänge geöffnet), die den Rechner des Empfängers mit Ransomware infizieren oder als Sprungbrett für größer angelegte Angriffe auf Unternehmensnetzwerke missbrauchen, mit denen große Geldsummen erpresst werden sollen.

Entsprechend kann bereits ein einzelner, gut konfigurierter Spamfilter eine wichtige erste Verteidigungslinie gegenüber Ransomware sein. Viele Unternehmen haben einen solchen bereits im Einsatz, war es doch auch

schon vor großangelegten Ransomware-Attacken wie den aktuellen sinnvoll, Mitarbeiter vor Spam und Phishing zu schützen.

Von großem Vorteil kann zusätzlich sein, jede Art von Anhängen zu blockieren, die in Ihrem Unternehmen im Allgemeinen nicht verwendet werden. Wie praktikabel diese Herangehensweise ist, hängt natürlich vom Unternehmen ab und erfordert möglicherweise umfassendere Prozessänderungen. Beispielsweise kann es sein, dass Ihre Mitarbeiter gewohnt sind, einander Excel- und Word-Dateien per E-Mail zu schicken. Die Umstellung auf eine File-Sharing-Lösung kann sinnvoll sein, stößt aber eventuell auf Widerstände, mit denen umgegangen werden muss.

Eine weitere Maßnahme kann sein, eine leistungsfähige EPP (Endpoint Protection)-Software zu installieren und so Ihre Mitarbeiter daran zu hindern, potentiell Malware-verbreitende Webseiten zu besuchen. Auch ein Filter für Web-Content kann hier gute Dienste leisten, indem er bösartige Webseiten von vornherein blockiert.

Die EPP-Lösung sollte dabei zentral verwaltet sein, um Sicherheitsrichtlinien erfolgreich um- und durchsetzen zu können. So lässt sich beispielsweise verhindern, dass Mitarbeiter den Schutz eigenständig deaktivieren oder unbekannte Wechselmedien benutzen. Die EPP-Lösung ist dabei immer auf dem neuesten Stand zu halten. Verfügbare Cloud-Anbindungen sollten aktiviert werden, da so die Reaktion auf neuartige Bedrohungen wesentlich schneller möglich ist (ESET nennt seine Cloud-Anbindung LiveGrid).

Das rechtzeitige und umfassende Patchen von Betriebssystemen und Anwendungen hilft, Ransomware-Attacken zu verhindern. Auch durchdachte Sicherheitseinstellungen sind von nicht zu unterschätzender Bedeutung. Es kann zum Beispiel sinnvoll sein, Microsoft Office-Makros für bestimmte Nutzergruppen komplett zu deaktivieren um die Angriffsfläche für Ransomware weiter zu minimieren. Das macht natürlich nur dann Sinn, wenn Ihre Unternehmensabläufe nicht auf Makros angewiesen sind.

Es steht außer Frage, dass für die IT-Sicherheit eines Unternehmens alle ihren Beitrag leisten müssen. Entsprechend sollten diese laufend umfassend geschult und auf dem neuesten Stand sein. Ben Reed, *Cybersecurity Awareness-Trainer*, sagt dazu: „Die Anzahl an Malware-Vorfällen im Unternehmen lässt sich merklich verringern, wenn die Mitarbeiter darüber informiert sind, worauf sie bei Phishing- oder anderen Malware-E-Mails achten müssen."

Ihnen muss klar sein, dass sie bei verdächtigen Mails oder Attachments sofort den Helpdesk oder das Security-Team informieren müssen. So wird nicht nur verhindert, dass Malware ins Unternehmensnetzwerk gelangt. Frühwarnsysteme helfen auch, Spamfilter besser zu kalibrieren und Firewalls zu verbessern.

Lieferkette und „Drive-by"-Infektionen

Ein weiteres Einfallstor, welches nähere Betrachtung verdient, ist die Lieferkette von Softwareprodukten.

In den Anfangsjahren von Software und Malware verbreiteten sich Computerviren vor allem über Disketten, dem Hauptverkehrsweg legitimer Software. Entsprechend kam es vor, dass sich Malware bereits auf neu gekauften Disketten befand oder auf Disketten mit Probeversionen, wie sie häufig Computermagazinen beigelegt waren.

Der heutige Infektionsweg kann sehr ähnlich sein: Wie ESET-Forscher im letzten Jahr feststellten, nutzte zum Beispiel die *NotPetya/DiskCoder.C-Malware* eine legitime Buchhaltungssoftware, um in Systeme einzudringen. Die Angreifer kaperten den Update-Server des Herstellers und fügten dem legitimen Update-Code ihren schädlichen hinzu. Nutzer, die das Update installierten, installierten so auch eine Backdoor, mit deren Hilfe wiederum Ransomware auf ihr System gelangen konnte. Mithilfe leistungsfähiger Endpoint Protection-Produkte und EDR-Tools konnten Unternehmen sich hier jedoch effektiv schützen.

Beinahe ironische Ausmaße nimmt die Sache an, wenn ein ganz besonderer Abschnitt der Lieferkette von Software von Missbrauch betroffen ist: Cracking-Seiten, also solche Webseiten, die Informationen

und Codes zur illegalen kostenlosen Nutzung legitimer Software bereitstellen. 2018 berichtete *Bleeping Computer*, dass die GandCrab-Ransomware, welche ESET als *Win32/Filecoder.GandCrab* identifiziert, sich als Gratis-Download eines Cracking-Codes getarnt hatte.

In den letzten Jahren konnten Forscher zudem eine Zunahme von sogenannten „Drive-By" Angriffen, also Angriffen „im Vorbeigehen" beobachten, d.h. Infektionen von Webseitenbesuchern ohne dezidierten Dateidownload von der Seite. Ransomware, welche bei ESET unter der Bezeichnung Win32/Filecoder.Princess bekannt ist, verbreitet sich mit dieser Methode (Unser Dank geht an Malwarebytes Labs für die Entdeckung.). Hierfür platziert der Angreifer ein sogenanntes Exploit Kit auf einer Webseite. Dabei kann es sich um eine legitime aber gekaperte oder eine durch den Angreifer erstellte Webseite handeln. Besucht jemand eine Seite mit Exploit Kit, infiziert die Malware den Rechner des Opfers über verschiedene Schwachstellen, je nach Setup des infizierten Rechners. Verwendet dieser zum Beispiel einen ungepatchten Webbrowser, können bekannte Schwachstellen ausgenutzt werden. Die effektivste Abwehr gegenüber solchen Attacken ist es, Software stets aktuell zu halten, Endpoint Security-Lösungen zu installieren und Mitarbeiter anzuhalten, keine unbekannten Webseiten zu besuchen.

Clouds und Segmente

Unabhängig davon, welches Einfallstor eine Ransomware ausnutzt – hat sie es einmal in das Unternehmensnetzwerk geschafft, wird sie sehr wahrscheinlich versuchen, so viele Rechner wie möglich zu infizieren. Im oben erwähnten Fall von LabCorp waren mehrere Tausend Rechner innerhalb einer Stunde infiziert. Als NotPetya es schaffte, das Netzwerk des Logistik-Giganten Maersk zu infizieren, zog dies innerhalb kürzester Zeit *45.000 PCs und 4.000 Server* in Mitleidenschaft. Entsprechend erscheint es eine gute Strategie, die Anzahl der Rechner, die bei einer Attacke infiziert werden können, möglichst klein zu halten. Hierfür existieren verschiedene Ansätze - einer davon die Aufteilung des Netzwerks in Segmente.

Wir können hier natürlich nicht im Detail über Netzwerkarchitekturen sprechen. Interessierte Leser finden zum Beispiel in diesem *KPMG Report* weitere Informationen. Festzuhalten ist aber, dass die Segmentierung eines Netzwerks sich nicht ohne finanziellen und personellen Aufwand durchführen lässt. Unternehmen sollten dennoch um die Vor- und Nachteile ihrer aktuellen Netzwerkarchitektur wissen, um sie gegebenenfalls optimieren zu können. Schon ein einfaches, interviewbasiertes Audit kann hier wichtige Einblicke geben. Grundlegende Fragen, die dabei gestellt werden sollten, sind beispielsweise „Wie komme ich von hier nach dort?" und „Wie wird verhindert, dass jemand von dort nach hier kommt?"

Wären diese Fragen vor November 2013 bei Target gestellt worden, hätte vielleicht verhindert werden können, dass eine Phishing E-Mail mit einem Trojaner, die vom Mitarbeiter eines Heizungs- und Sanitär-Dienstleisters des Einzelhandels-Giganten geöffnet worden war, bis zu den Kassensystemen hätten vordringen können. Wäre auf demselben Verbreitungsweg Ransomware installiert worden, wäre der Schaden für Target wohl wesentlich größer ausgefallen als „nur" der großangelegte Diebstahl von Kreditkartendaten.

In den letzten Jahren hat die Beliebtheit cloudbasierter Systeme auch in der EU stark zugenommen. Die Architektur von Netzwerken lässt sich so „in die Breite" ziehen, Daten werden extern gelagert. Dies jedoch bietet natürlich in sich keinen Schutz gegenüber Ransomware, auch wenn unseriöse Anbieter dies zum Teil behaupten. Aufgrund der geringen Kosten, die das Aufsetzen eines Cloud-Servers verursacht, drängen viele Anbieter in den Markt – und vernachlässigen vielfach die Sicherheit. Entsprechend sind Cloud-Server selbst für Kriminelle zu äußerst attraktiven Zielen geworden. Der bereits erwähnte Angriff auf das CDOT begann mit einem virtuellen Server, der bereits nach zwei Tagen per Brute Force infiziert worden war. Eines ist klar: Die Auslagerung von Unternehmens-IT in die Cloud erfordert hieb- und stichfeste Sicherheitskonfigurationen. Ebenso muss auch die Cloud in umfassende Backup- und Wiederherstellungsframeworks eingebunden werden.

Patching und Backups als Schutz vor Ransomware

Wie schon erläutert, sind regelmäßige Updates und Backups zentral für die Abwehr von Ransomware. Updates und Patches stellen sicher, dass Schwachstellen geschlossen sind oder dass Ransomware, schafft sie es dennoch einzudringen, zumindest nur geringen Schaden anrichten kann. So patcht das Windows Security Bulletin MS17-10 z.B. Windows SMB, schützt so vor EternalBlue und dämmt die Verbreitung von NotPetya und WannaCryptor wirksam ein.

Dabei ist jedem Systemadministrator wohl schmerzlich bewusst, dass Patching eine komplexere Aufgabe sein kann als es auf den ersten Blick scheint. Patches und Updates müssen getestet werden, bevor sie auf die Systeme aufgebracht werden, um beispielsweise Einblick in Abhängigkeiten von Anwendungen oder des Betriebssystems zu bekommen, die durch Updates gestört werden könnten. Der Aufwand erscheint jedoch gerechtfertigt, bedenkt man die Unsummen, die Ransomware-Angriffe ein Unternehmen kosten können.

Eines ist klar: Ein durchdachtes und sorgfältig verwaltetes Backup- und Wiederherstellungssystem ist die wirksamste Gegenmaßnahme, falls es Ransomware – auf welchem Weg auch immer – doch einmal ins Unternehmensnetzwerk schaffen sollte. Dabei ist aber immer auch zu bedenken, dass Ransomware-Angriffe über einen längeren Zeitraum ablaufen können und in dieser Zeit entsprechend auch Backups von sich erstellen und so eine Wiederherstellung erschweren. Backups sind keineswegs eine statische Verteidigungslinie. sie müssen fortlaufend überwacht und verwaltet werden. Der Wiederherstellungsprozess muss außerdem regelmäßig getestet werden.

Glücklicherweise sind die Möglichkeiten für Backup und Wiederherstellung aktuell vielfältiger denn je – vor allem dank der Möglichkeit, Daten in die Cloud zu verlagern. Im Gegenzug gibt es jedoch auch so viele Daten wie nie zuvor, die von immer vielfältigeren Orten aus gesichert werden müssen. Den Backup-Experten von Xopero zufolge umfasst eine gute Backup-Strategie alle Daten und Systemzustände auf allen Endpoints, Servern, E-Mail-Postfächern, Netzlaufwerken, Mobilgeräten und VMs.

Hier ausführlich auf Maßnahmen einzugehen, würde den Rahmen dieses Papiers sprengen. Dennoch sollte klar sein, dass eine solche Strategie heute wichtiger ist denn je. Ransomware ist dabei nur ein Punkt in einer langen Liste von Gründen, warum Unternehmen dieses Element ihrer IT-Infrastruktur keineswegs vernachlässigen sollten. Wie David Harley, ESET Senior Research Fellow in *Trends 2018: The cost of our connected world* im Abschnitt „The ransomware revolution“ verdeutlicht, gibt es gute Gründe, beim Planen von Backups genau zu überlegen: „Sind Datenspeicher ‘always on‘, können ihre Inhalte leicht durch Ransomware angegriffen werden, genauso wie lokale und andere mit dem Netzwerk verbundene Datenspeicher.“ Harley empfiehlt Offsite-Speicher, die

- nicht dauerhaft und unhinterfragt online sind,
- Daten sichern und
- umfassend vor unbemerkter Modifikation schützen,
- mehrere, ältere Backup-Versionen speichern, sodass selbst bei Zerstörung jüngerer Backups zumindest einige Daten wiederhergestellt werden können,
- Kunden absichern, indem genau dargelegt wird, welche Pflichten der Server-Provider innehat, was geschieht, wenn er insolvent wird usw.

Harley meint zudem, dass nicht wiederbeschreibbare Medien ein sehr nützliches und einfaches Mittel zur Archivierung von Daten sein können, da sie kaum durch Ransomware infiziert werden können.

Zusätzlich gibt es natürlich unzählige weitere Gründe, warum Ihr Unternehmen ein umfassendes Sicherungssystem implementieren sollte – Naturkatastrophen sind nur einer davon.

Und wie reagiert man nun auf Ransomware?

Sich vor dem Eindringen von Ransomware abzusichern, reicht natürlich nicht aus. Jedes Unternehmen muss auch in der Lage sein, auf Schadsoftware zu reagieren, die es allen Abwehrstrategien zum Trotz in das Netzwerk geschafft hat. Basis bilden hier erneut Sicherheitspolicys, die für das gesamte Unternehmen auf allen Ebenen gelten und regelmäßig entsprechend der neuesten Bedrohungen aktualisiert werden. Die Richtlinien sollten folgende Fragen beantworten:

- Wer ist zu benachrichtigen, wenn Mitarbeiter verdächtige Dateien oder Vorgänge beobachten?
- Wie wird mit Lösegeldforderungen umgegangen?
- Wer ist verantwortlich für eventuelle Zahlungen/Zahlungsverhandlungen in Bezug auf Lösegelder? Ziel ist dabei, folgende Probleme zu vermeiden:
- Mitarbeiter melden Vorfälle nicht aus Angst vor negativen persönlichen Konsequenzen,
- Netzwerk-Admins zahlen Lösegelder, um langwierige und nervenaufreibende Wiederherstellungsprozesse zu umgehen,
- Die Öffentlichkeit erfährt unkontrolliert von tatsächlichen oder vermeintlichen Ransomware-Angriffen auf das Unternehmen.

Nachdem die Sicherheitsrichtlinien in Bezug auf Ransomware aktualisiert worden sind, muss sichergestellt werden, dass auch Security Awareness-Prozesse und Trainingsprogramme Ransomware thematisieren.

Ebenso sollte dafür gesorgt werden, dass der Krisenreaktionsplan auf eine Ransomware-Attacke vorbereitet ist. Er sollte mindestens folgende Punkte umfassen:

- Bei ersten Hinweisen auf einen Angriff sind die entsprechenden Verantwortlichen zu kontaktieren.
- Betroffene Rechner sind zu isolieren und genau zu untersuchen.
- Kann bestätigt werden, dass es sich um eine Attacke handelt, muss das Incident/Crisis Response-Team aktiviert werden.
- Die Rechtsabteilung ist zu informieren.
- Zulieferer, die Unterstützung leisten könnten, sollten kontaktiert werden.
- Mitarbeiter sind an Geheimhaltungspflichten gegenüber der Presse und in sozialen Medien zu erinnern.
- Der Umfang des Angriffs und die Eigenschaften der Ransomware müssen identifiziert werden (z.B. anhand des Keys, wenn bekannt).
- Die Polizei ist zu informieren.
- Eine Pressemitteilung muss erstellt werden.
- Wurden Daten verschlüsselt, ist zu klären, ob diese aus dem Backup wiederherzustellen sind.
- Mitarbeiter sind auf den neuesten Stand bezüglich der Entwicklungen zu bringen.
- Wenn nötig, muss der Business Continuity-Plan zum Einsatz kommen.

Es kann hilfreich sein, zumindest ein Ransomware-Szenario im Krisenplan unterzubringen und es mit den relevanten Mitarbeitern durchzuspielen. So lassen sich am ehesten Lücken im Plan identifizieren. Gleichzeitig wird für alle deutlich, was genau passiert, wenn selbst grundlegende Arbeitsmittel nicht nutzbar sind (E-Mail, Internetzugang, VoIP-Telefonie).

Endpoint Detection and Response (EDR)

Mithilfe von speziellen Tools lässt sich die Abwehr von Ransomware und ihren Folgen wesentlich vereinfachen. Endpoint Detection and Response (EDR)-Tools automatisieren einige Mechanismen der Ransomware-Abwehr und unterstützen so Sicherheitsverantwortliche umfassend. Abbildung 4 zeigt einige EDR-Regeln, mit deren Hilfe verdächtige Aktivitäten, die auf Ransomware-Angriff hindeuten, frühzeitig erkannt werden können. (Beim hier dargestellten EDR-Tool handelt es sich um den *ESET Enterprise Inspector, der im Laufe des Jahres 2019 auch im deutschsprachigen Markt verfügbar sein wird.*)

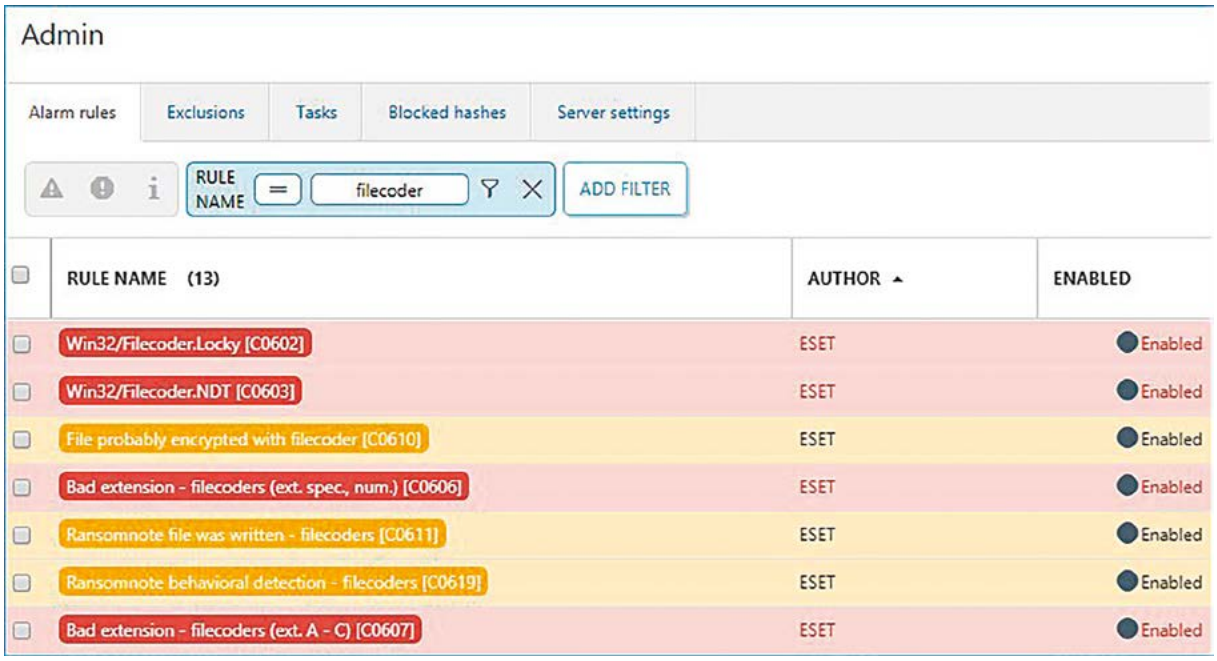

Abbildung 4

Mithilfe eines EDR-Tools lassen sich alle Endpoints in Ihrem Unternehmensnetzwerk auf verdächtige Aktivitäten untersuchen, z.B. die Änderung von Dateinamen.

Dieses Verhalten zeigen zum Beispiel Mimikatz, welches Nutzerdaten stiehlt und xDedicRDPPatch, welches zusätzliche Nutzeraccounts erstellt, wenn ein Server via RDP kontaktiert wird (erhältlich über die bereits erwähnte xDedic-Webseite).

Anzeichen schädlicher Aktivitäten im Netzwerk lassen sich mithilfe gut durchdachter Regeln und Alarme frühzeitig erkennen. Derartige Regeln können laufend mit neuen Informationen, z.B. IoCs (Indicators of Compromise) aktualisiert werden. Mithilfe eines guten EDR-Tools können Admins den betroffenen Rechner schnell identifizieren, isolieren und das Problem diagnostizieren. Dazu gehört auch, die Befehle, die das infizierte System bis dahin ausgeführt hat, nachzuvollziehen. So unterstützt ein EDR-Tool Sicherheitsteams umfassend bei der Abwehr und Analyse von Angriffen.

Ein Wort zum Thema Lösegeld

Die Antwort auf die Lösegeldfrage in Bezug auf Ransomware lautet schlicht: nein.
Bezahlen Sie den Kriminellen, die Ihre Daten verschlüsselt haben, Lösegeld,

- unterstützen Sie damit deren Geschäftsmodell,
- finanzieren Sie letzten Endes kriminelle Aktivitäten,

- können Sie nicht mit Sicherheit sagen, dass Folgeforderungen und weitere Angriffe ausbleiben werden.

Sie wissen nicht einmal sicher, dass die Kriminellen Ihnen den Entschlüsselungs-Key geben werden. Und selbst wenn sie es tun, garantiert das nicht, dass Ihre Daten komplett entschlüsselt werden können. Hierfür können mehrere Punkte verantwortlich sein:

- Die Ransomware ist fehlerhaft programmiert oder
- der Entschlüsselungs-Key wird nicht korrekt übertragen.
- Nicht zuletzt kann es natürlich immer auch sein, dass der oder die Angreifer nie beabsichtigten, die Daten wieder freizugeben.

Unternehmen fühlen sich vor allem dann verpflichtet, Lösegelder zu zahlen, wenn sie sich nicht in der Lage sehen, die Daten aus Backups wiederherzustellen, z.B. weil es keine Backups gibt oder weil diese in irgendeiner Weise kompromittiert sind. Es gibt aber Alternativen zum Zahlen des Lösegeldes: *David Harley empfiehlt daher:* „Bevor Sie auf die Lösegeldforderung eingehen, sollten Sie prüfen, ob nicht eventuell Ihr Sicherheitsanbieter helfen kann, die Daten wiederherzustellen. Selbst wenn dies nicht möglich ist, kann er Ihnen sagen, ob es sich bei der vorliegenden Ransomware womöglich um eine Variante handelt, bei der die Täter auch nach Zahlung des Lösegeldes die Daten nicht entschlüsseln."

Ein weiteres mögliches Argument, das Lösegeld doch zu zahlen ist die Annahme, dass dies weniger Kosten verursachen würde, als die Daten wiederherzustellen. Dass es sich hier jedoch um eine Milchmädchenrechnung handelt, dürfte nach den oben genannten Argumenten klar sein.

Vermutlich haben Sie von Ransomware gehört, die Beweise dafür verspricht, dass die Entschlüsselung funktioniert. Das kann tatsächlich zu noch weitreichenderen Problemen führen, wie sich erst kürzlich im Fall des Datenlecks bei *HMC* eindrücklich zeigte: Senden Sie eine verschlüsselte Datei an den Angreifer, um sie entschlüsseln zu lassen, geben Sie ihm damit zugleich Zugriff auf potentiell sensible Daten.

Die Zukunft der Ransomware

Mit zunehmender Abhängigkeit von Unternehmen von Technologie wächst auch die Angriffsfläche für Ransomware. Entsprechend können wir davon ausgehen, dass Ransomware weiterhin bestehen und sich weiterentwickeln wird.

30 Jahre Erfahrung im IT-Security-Bereich ließen uns folgende Evolutionsschritte von Malware beobachten:

- Schwachstellen einer neuen Technologie werden entdeckt und ihr Potential für Missbrauch ausgelotet;
- Maßnahmen zum Schließen der Schwachstelle werden in Angriff genommen;
- Versuche, die Technologie zu missbrauchen sind zunächst recht selten, da Kriminelle genug mit bestehenden Einfallstoren verdienen;
- ohne tatsächliche Attacken „in freier Wildbahn" nimmt das Interesse an Gegenmaßnahmen ab;
- Kriminelle entdecken die „neue" Technologie schließlich doch für sich und beginnen, sie großflächig anzuwenden;
- ein neuer Malware-Trend zeichnet sich ab.

Entsprechend lief beispielsweise die Entwicklung von DDoS-Attacken, z.B. *Mirai* und die Router-Malware *VPNFilter*, ab. Ransomware profitiert aktuell vom Trend hin zu (oft schlecht gesicherten) IoT-Geräten und industriellen Steuerungssystemen mit Internetzugang sowie „smarten" Gebäuden und Fahrzeugen (darunter autonome Fahrzeuge, siehe auch den Artikel *„RoT: Was ist Ransomware of Things"*).

Sollten Kriminelle mit den aktuell verfügbaren Methoden nicht mehr genügend Geld verdienen können, sind folgende Szenarios denkbar: Router-Malware könnte den Traffic drosseln oder gänzlich sperren bis ein

Lösegeld bezahlt wurde; sie könnte drohen, den Router komplett unbrauchbar zu machen oder ankündigen, Traffic-Inhalte zu veröffentlichen, sollte versucht werden, die Malware zu entfernen.

Weiterhin könnten Fahrzeuge, Wohnungen und Gebäude aus der Ferne gesperrt werden, um Lösegeld zu erpressen. Steuerungssysteme von Heizungen, Klimaanlagen usw. sind ebenfalls lohnenswertes Ziel für Erpressungsversuche (und werden es in Ansätzen auch schon). Dass kommerziell genutzte Roboter ein Ziel für Malware-Angriffe sein können, wurde ebenfalls bereits gezeigt.

Für Unternehmen ergeben sich aus diesen Entwicklungen verschiedene Implikationen. Folgende Vorgehensweise wird empfohlen:

- potentielle Gefahren müssen in den Risikomanagement-Plan aufgenommen werden;
- mögliche Ransomware-Ziele im Unternehmen, d.h. IoT-Geräte, SOHO-Router, Roboter, Steuerungssysteme, autonome Systeme sind zu identifizieren und zu dokumentieren;
- Schwachstellen sind zu dokumentieren;
- besonderes Augenmerk ist auf Patches und Updates zu legen;
- IoT-Geräte und ähnlich „neue" Assets sollten von produktiven Netzwerken abgekapselt werden.

Wenn Ihr Unternehmen diese Hinweise befolgt, schützen Sie sich zugleich gegenüber anderen Malware-Trends wie dem bereits besprochenen Kryptomining. Wir haben ebenso bereits darüber gesprochen, dass Malware nur selten einzeln auftritt. So ist zu erwarten, dass in der Zukunft Kombinationen aus Ransomware und Kryptomining zu beobachten sein werden. Infizierte Systeme könnten beispielsweise so lange gesperrt werden, bis eine bestimmte Summe Kryptowährung geschürft worden ist. Denkbar ist auch, dass die IT-Infrastruktur eines Unternehmens so lange für das Mining missbraucht wird, bis ein Lösegeld gezahlt worden ist.

Fazit

TDer Kampf gegen Malware, die versucht, Technologie für kriminelle Zwecke zu missbrauchen, geht unablässig weiter. Finanziell gut ausgestattete Kriminelle, Aktivisten sowie Regierungsorganisationen und nicht zuletzt das prototypische „Hacker-Kid", das die Konsequenzen seines Handelns nicht durchdacht hat, stehen Unternehmen gegenüber, die sensible und persönliche Daten vor unerwünschtem Zugriff und kriminellen Machenschaften schützen wollen.

Um in diesem Kampf nicht unterzugehen, ist es unabdingbar, so viel wie möglich über die Angreifer und ihre jeweils aktuelle Methodik zu wissen. Mit der Weiterentwicklung von Malware müssen auch Abwehrstrategien sowohl auf personeller als auch auf technologischer Ebene stets angepasst werden:

Neben umfassender Schulung der Mitarbeiter gehören zu einer vernünftigen Abwehr Sicherheitsrichtlinien und ihre Umsetzung, Sicherheitsprodukte und -tools (inklusive Backup- und Wiederherstellungssysteme) und ein stets aktueller Incident Response-Plan. Natürlich bietet auch das keine vollständige Sicherheit – die negativen Folgen von Angriffen können jedoch maßgeblich verringert werden.

Wir hoffen, dass unsere Ausführungen ihren Beitrag leisten, die Welt nicht nur komfortabler, sondern auch sicherer zu machen.

Anhang A:

Mit zunehmender Verfügbarkeit von gestohlenen Zugangsdaten im Dark Web nehmen Ransomware-Angriffe per RDP immer weiter zu. Abbildung A1 zeigt wie einer dieser Märkte, Ultimate Anonymity Services (UAS), für einen potentiellen Käufer aussieht, der Admin-Rechte auf einen RDP-Server in Florida erhalten möchte.

Besonders spannend ist hier, dass Kaufinteressenten die Auswahl ihrer Opfer gezielt einschränken können.

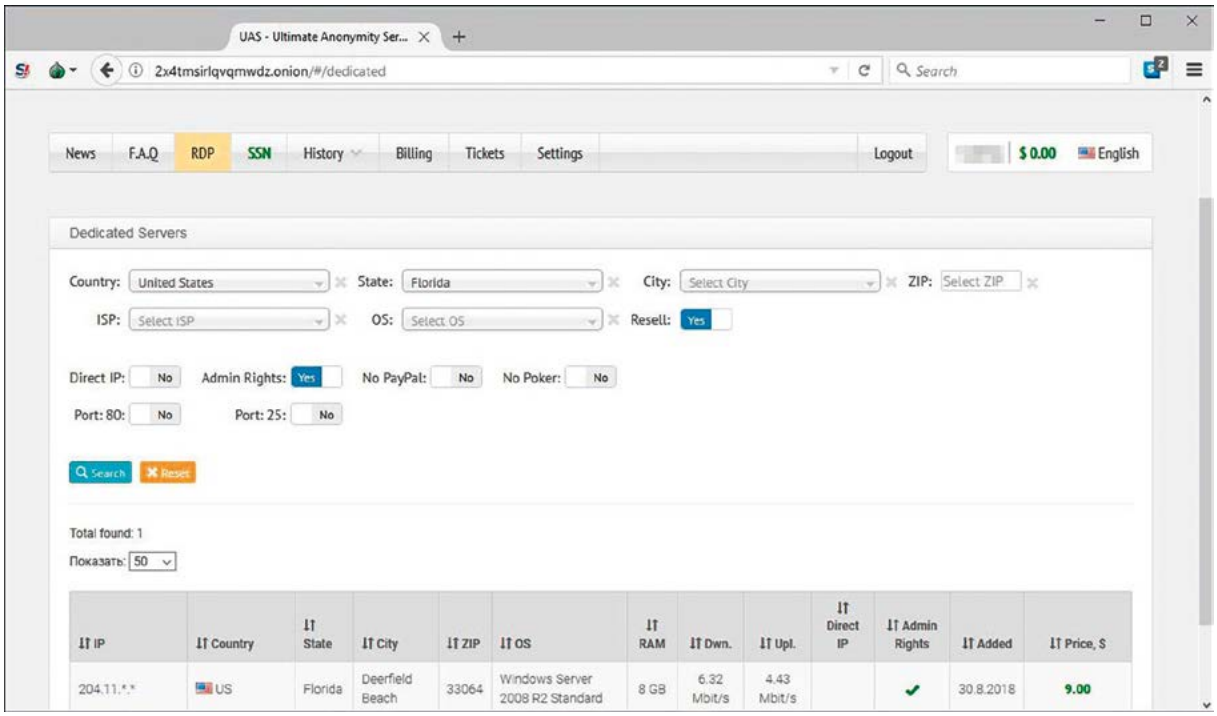

Abbildung A1

Beeindruckend ist auch die Vielzahl an Details, die zum aufgeführten „Artikel" angezeigt werden. Der Preis von 9$ ist im Vergleich zum größeren Marktplatz xDedic günstig. Seit Eröffnung der Seite 2014 waren hier hunderte Verkäufer von Zugangsdaten aktiv, also Hacker, die Server knacken und die Zugangsdaten verkaufen.

XDedic war dabei keineswegs schon immer Teil des Dark Web, sondern wurde erst nach Nachforschungen und Veröffentlichungen von Sicherheitsexperten dorthin verschoben. Heute müssen Kriminelle 200$ allein für den Zugang zu xDedic zahlen und ein Pfand von 50$ hinterlegen, welches einbehalten wird, wenn nicht innerhalb von 30 Tagen eine Transaktion zustande kommt.

Ähnlich wie UAS bietet auch xDedic umfassende Filterfunktionen.

Abbildung A2 zeigt, wie sich xDedic einem Kaufinteressenten präsentiert, der IP-Adresse und Adminrechte für Server im US-Bundesstaat New York kaufen möchte.

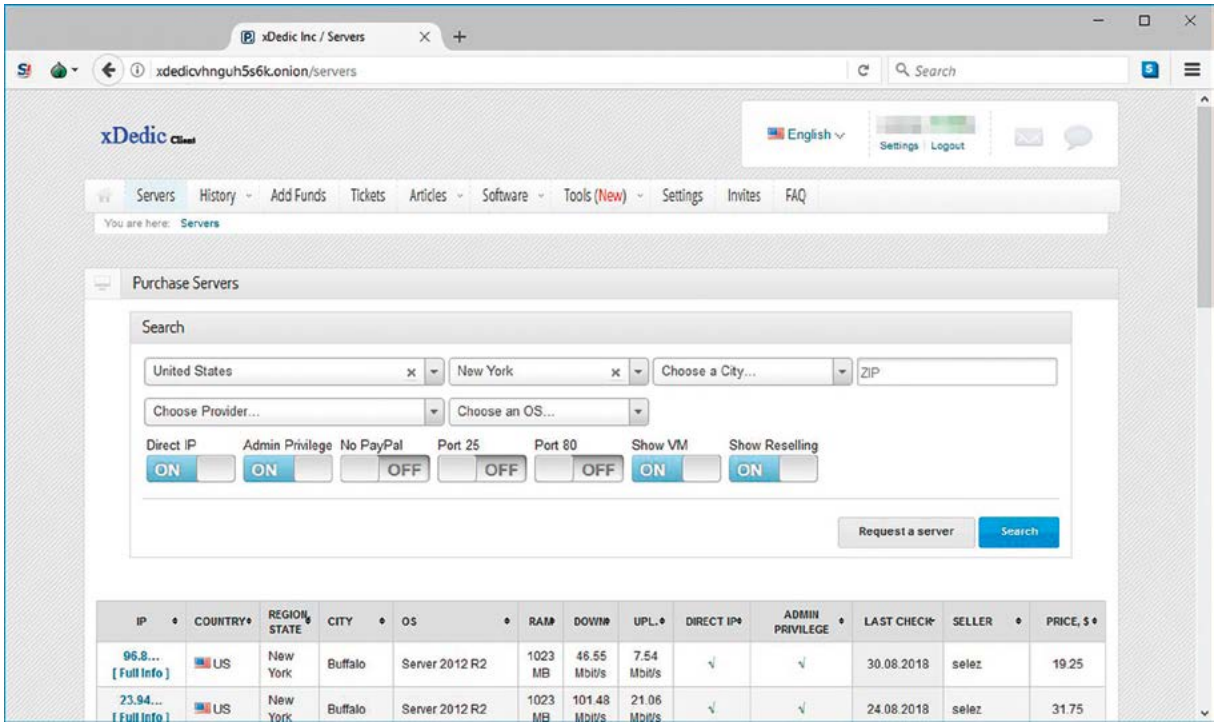

Abbildung A2

Auch hier bekommt der potentielle Käufer eine Vielzahl von Details präsentiert, bevor er seine Kaufentscheidung fällt. Natürlich werden die IP-Adressen nicht ohne Bezahlung angezeigt, man kann aber in Erfahrung bringen, wo der Rechner gehostet ist, seine Spezifikationen sowie die Geschwindigkeit seiner Internetverbindung abfragen und erfahren, ob es sich um eine virtuelle Maschine handelt. Ebenso erfährt der Käufer, ob der Rechner durch Anti-Malware geschützt ist und ob die IP-Adresse durch Anti-Spam und Anti-Malware-Hosting Organisationen geblacklistet ist. Alle Informationen werden übersichtlich in einem Pop-Up-Fenster dargestellt, siehe Abbildung A3.

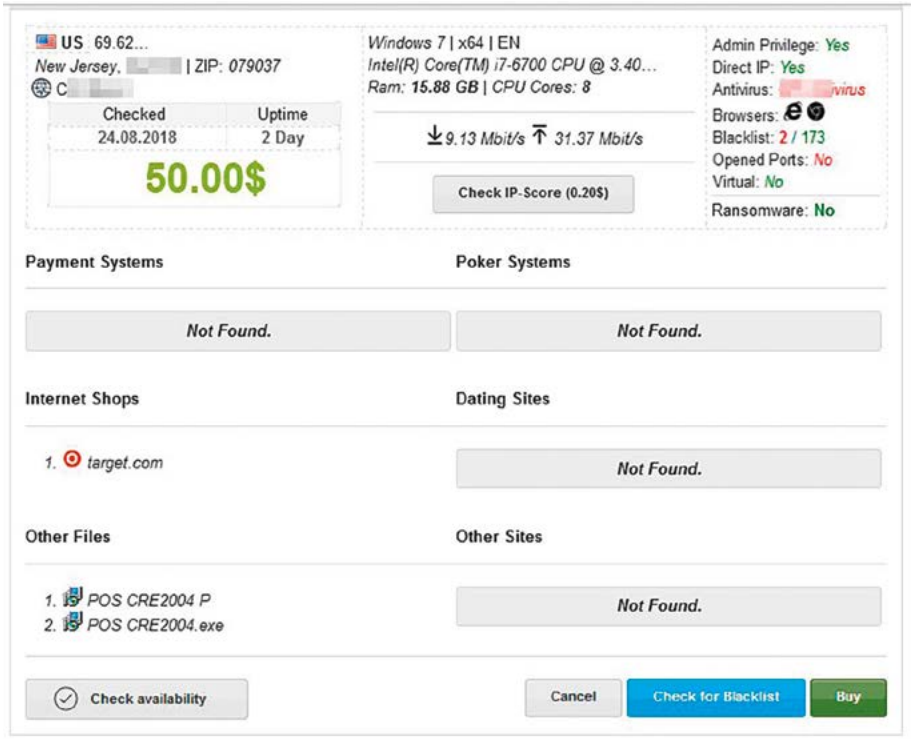

Abbildung A3

Anhang B: RDP gegen Ransomware absichern

Strategieempfehlungen und mögliche Techniken

1. Problemdokumentation

Stellen Sie sicher, dass alle mit dem Internet verbundenen Geräte den Sicherheitsverantwortlichen bekannt sind. Setzen Sie einen Prozess auf, der auch neue Geräte beinhaltet.

2. Angreifbare Assets auflisten

Stellen Sie sicher, dass keine Geräte direkt per Internetverbindung kontaktiert werden können, es sei denn, sie wurden für diesen Zweck freigegeben und entsprechend konfiguriert. Wenn möglich, sollten Verbindungen nur über VPN möglich sein.

Deaktivieren Sie RDP, wenn es nicht benötigt wird. (Informationen, wie das bewerkstelligt wird, finden sich hier: *Server 2016*; *Server 2008/R2*; *Windows 10*; *Windows 8*; *Windows 7*; *Windows XP*)

3. Angreifbare Assets absichern

Wenn Sie RDP unbedingt ohne VPN nutzen müssen, sollten Sie möglichst viele der folgenden Maßnahmen implementieren:

a. Ändern Sie das werksseitig gesetzte Passwort umgehend.

b. Verstärken Sie das Passwort (Länge, Zeichenmix etc.).

c. Legen Sie eine Anzahl an fehlgeschlagenen Logins fest, nach der der Account automatisch für eine bestimmte Zeit gesperrt wird.

So stellen Sie sicher, dass Angreifer mit entsprechenden Werkzeugen das Passwort nicht automatisch und per Brute Force erraten können. In Windows legen Sie dies folgendermaßen fest:

Gehen Sie auf „Start“ --> „Programme“ --> „Systemsteuerung“ --> „Lokale Sicherheitseinstellungen“. Unter „Verwaltung“ --> „Anmeldeversuche überwachen“ finden Sie drei Optionen. Setzen Sie für alle die Anzahl der möglichen Fehlversuche auf 3 und die folgende Sperrzeit auf 3 Minuten, sind Sie auf der sicheren Seite.

d. Verwenden Sie die Authentifizierung auf Netzwerkebene, um die Sicherheit des Host-Servers der Session zu erhöhen. So wird vor Erstellung der Session die Authentifizierung des Nutzers gegenüber dem Host-Server gefordert.

e. Ändern Sie den Standardport 3389 für RDP. (Vorsicht: Hierbei handelt es sich lediglich um einen „Tarnmechanismus“. Es sollte auf keinen Fall die einzige Schutzmaßnahme sein, die Sie implementieren.)

Um den Port zu ändern, modifizieren Sie folgenden Registry-Eintrag: (Achtung: dies sollte nur von Nutzern mit Kenntnis der Windows Registry und TCP/IP durchgeführt werden): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

f. Legen Sie fest, welche IP-Adressen sich via RDP verbinden können. (Dies kann allerdings eine langwierige Aufgabe sein, wenn Ihre Nutzer keine statischen IP-Adressen haben, z.B. weil sie von zuhause oder unterwegs arbeiten.)

g. Verwenden Sie mehr als einen Faktor für die Authentifizierung. Die Faustregel für mögliche Faktoren lautet „etwas, das man weiß (z.B. Nutzername und Passwort), etwas, das man ist (z.B. Fingerabdruck oder Stimme) und etwas, das man hat (z.B. Smartphone, mit dem Einmalpasswörter empfangen werden können)“.

Vermeiden Sie aber, SMS als Authentifizierungsfaktor zu verwenden. Diese wurden bereits mehrfach missbraucht (siehe *hier*). Es gibt viele gute 2FA-Lösungen auf dem Markt, die ohne SMS und trotzdem mit einer Vielzahl von Telefonmodellen funktionieren (z.B. *die 2FA von ESET*).

h. Verschärfen Sie Zugriffs- und Rechtebeschränkungen. Dateien sollten nicht aus AppData und LocalAppData oder dem Unterverzeichnis von AppData, Temp, gestartet werden können. Ebenso sollten ausführbare Dateien nicht aus den Arbeitsverzeichnissen verschiedener Entpackprogramme (WinZip, 7-zip) heraus ausgeführt werden können. Mithilfe eines guten Endpoint Protection-Produkts können Sie zudem HIPS-Regeln erstellen, die nur bestimmten Anwendungen erlaubt, auf dem Rechner ausgeführt zu werden. Andere werden automatisch blockiert.

i. Setzen Sie ein Passwort für Ihre Endpoint Protection-Lösung, um unerlaubte Änderungen von Einstellungen oder gar eine Deaktivierung/Deinstallation zu verhindern. (Natürlich sollte dieses Passwort ein anderes sein als das, welches Sie für Ihren RDP-Login verwenden.)

ÜBER ESET

Seit mehr als 30 Jahren entwickelt *ESET®* beste Sicherheitslösungen und Services für IT-Infrastrukturen und schützt so Unternehmen wie Privatkunden weltweit umfassend vor zukünftigen Bedrohungen. Das Portfolio umfasst Sicherheitslösungen für Endpoints und Mobilgeräte sowie Verschlüsselung und Zwei-Faktor-Authentifizierung. ESET bietet maximale Performance bei minimalem Ressourcenbedarf und sorgt so für umfassende Sicherheit, ohne Arbeitsabläufe zu beeinträchtigen.

Die Gefahrenlandschaft entwickelt sich stetig weiter – und wir auch. Dank unserer F&E-Zentren auf der ganzen Welt waren wir der erste Anbieter von IT-Sicherheit, der 100 Virus Bulletin Awards in Folge für sich verbuchen konnte. Weitere Informationen finden Sie auf www.eset.de sowie LinkedIn, Xing, Facebook und Twitter.

ENJOY SAFER TECHNOLOGY™