NT4 ADMINS

MAGAZIN

12 2016

01 2017

Dezember 2016 – Januar 2017

Inhalt

Editorial

Florian Huttenloher
Technische Leitung
Florian.huttenloher@nt4admins.de

Der Hackerkongress „33C3“ hat es gezeigt: Attacken auf die IT-Infrastruktur der Unternehmen werden immer besser vorbereitet. Dabei bedienen sich die Angreifer aus einem großen Portfolio. Würmer, Viren, Erpressungstrojaner, DDoS-Angriffe und die Ausnutzung von (noch) unbekannten Sicherheitslücken gehören zum „Handwerkszeug“. Auch immer genauer zugeschnittene E-Mails mit Schadsoftware – oftmals mittels Makros in Office-Dokumenten – erreichen in den Abteilungen der Firmen ihre Opfer. Diese „Social-Engineering-Masche“ ist zwar seit langem bekannt, wird aber durch eine entsprechende Anpassung an die Erwartungshaltung der Empfänger erfolgreich eingesetzt. Um hier gegenzusteuern, stellt das Team von NT4ADMINS unterschiedliche Lösungsansätze vor – auch WaaS kann hierbei hilfreich sein.

Florian Huttenloher

IT-Sicherheit: Die Basics verstehen

Um die Sicherheit im IT-Bereich zu gewährleisten, steigen die Anforderungen für die Unternehmen regelmäßig. So gilt es immer neueren Bedrohungen zu wiederstehen, Angriffe abzuwehren, Schadsoftware zu neutralisieren oder Social-Engineering-Attacken vorzubeugen. Dabei sind sowohl reaktive, als auch proaktive Strategien verfügbar. Vom klassischen Ansatz, Netzwerkfirewall und Virenschutzlösungen, bis hin zur „aktiven" Gegenmaßnahmen an den Servern du Clients sind viele Details zu beachten. Aber auch die „Sicherheitslücke Mitarbeiter" sollte mit der entsprechenden Aufmerksamkeit bedacht werden.

In letzter Zeit wurden vermehrt direkte Angriffe auf die Geschäftsdaten von Großunternehmen bekannt. Dabei zielen die Angreifer häufig auf Datensätze mit sensiblen Dateien, meist persönliche Informationen der jeweiligen Unternehmenskunden. Dazu gehören zum Beispiel Kreditkarteninformationen, Sicherheitsnummern, Namen und Adressen, Geburtsdaten und ähnliche Details. Nachdem Großunternehmen (meist) ein vergleichsweise riesige" Datenbank für Millionen von Einzelkunden im Betrieb haben, loht sich diese Art der IT-Kriminalität anscheinend. Selbst wenn die Angriffe „nur" bezwecken, Datensätze zu stehlen, und diese an Dritte gegen Bezahlung weiterzugeben, ist an dieser Stelle einiges an Profit zu erwarten.

Aber nicht nur „die Großen" werden Opfer von Angriffen oder Malware. Auch Kleine und Mittlere Unternehmen und teilweise Privatpersonen werden – mehr oder weniger gezielt – angegriffen. Dabei sind weder die Unternehmens-Server, Desktop-Clients oder kleinere Systeme (Laptops, Mobilgeräte wie Tablets oder Smartphones) vor diesen kriminellen Subjekten „sicher".

Umso wichtiger ist es für die Unternehmen, entsprechende Gegenmaßnahmen zu ergreifen. Zum einen sollte eine möglichst hohe Resistenz gegen Angriffe von außen aufgebaut werden. Auch auf Sicherheitslücken von „innen" ist dabei zu achten, etwa wenn Mitarbeiter sensible Daten mit nach Hause – oder schlimmer noch – auf ungesicherte Cloud-Lösungen übertragen. Nachdem selbst mit dem größten Aufwand keine einhundertprozentige Sicherheit erreicht werden kann, ist es umso wichtiger, den Schaden bei einem Angriff zu begrenzen. Etwa wenn innerhalb des Unternehmens weitere Sicherheitsschranken eingerichtet werden. Dies kann etwa mit einem ausgefeilten Berechtigungs-System, oder entsprechenden Netzwerksegmentierungen erreicht werden.

Auch sollten die Überwachungsfunktionen, Log- und Protokolldateien, sowie bei Bedarf weitere Security-Lösungen die Systembetreuer dabei unterstützen, bereits laufende Angriffe zu erkennen. Denn wenn der „äußere" Verteidigungsring einmal „geknackt" wurde, versuchen die Angreifer (in beinahe allen Fällen) sich im System weiter zu verbreiten, um letztendlich Zugriff auf alle Informationen und Systeme im Netzwerk zu erlangen. Solch ein Vorgehen kann meist mit den entsprechenden Kontrollfunktionen aufgedeckt werden.

Im Anschluss daran können die Administratoren versuchen die Angreifer zu identifizieren, und die entsprechenden Beweise (etwa Schadsoftware oder gekaperte Administrator-Benutzerkonten) forensisch zu dokumentieren. Im Anschluss daran sollten gezielt Gegenmaßnahmen ergriffen werden, um noch laufende Angriffe aktiv zu bekämpfen. Hier spielt oftmals das sehr wichtige Thema „Backup" eine entsprechende Rolle, beispielsweise wenn „virenverseuchte" System bereinigt werden sollen.

Im Anschluss sollten die Unternehmen einen Lernprozess starten, um die entsprechenden Konsequenzen aus fehlgeschlagenen oder gelungenen Attacken zu ziehen. Unter Umständen müssen gewisse Kernkomponenten im Netzwerk getauscht werden, die Benutzerrechte neu strukturiert oder Mitarbeiterschulungen durchgeführt werden. Falls das noch nicht geschehen ist, sollten die Firmen auch externe Dienstleister heranziehen, um das eignen Netzwerk und IT-System samt den Mitarbeitern einer entsprechenden Prüfung zu unterziehen, Diese Art der aktiven Überprüfung wird von unterschiedlichen Firmen offeriert, meist im Rahmen eines Penetrationstest (Pentest). Die „Angreifer" bedienen sich dabei derselben Methoden, Werkzeuge und Tricks, die auch von den echten Kriminellen angewandt werden.

Perimeter-Verteidigung: der klassische Ansatz

Der erste Sicherheits-Checkpoint stellt in der Regel ein zuverlässiger Perimeter Schutz dar. Hierbei installieren die Unternehmen Firewall-Lösungen (auf Basis von Hardware-Appliances oder entsprechenden Softwarekomponenten), und versuchen auf diese Weise das interne Netzwerk „sauber zu halten". Zusätzlich werden, einzelne PC-Systeme der Mitarbeiter (Endpoints) mit entsprechenden Anti-Viren-Programmen zu versehen. Auch auf den Servern gehört es zum guten Ton" eine entsprechende Virenschutzlösung einzusetzen. Auf diese Weise lässt sich bereits ein relativ hoher Schutz erreichen, bekannte Malware wird (meisten) zuverlässig erkannt, und vernichtet. Der Nachteil: Eben nur bekannte Schadprogramme befinden sich in den (meist täglich aktualisierten) Virensignaturen, die der Hersteller zur Verfügung stellt. Unbekannte Schädlinge haben somit oftmals „freie Bahn".
Die Hersteller von Anti-Viren-Software hinken den Malware-Programmieren somit immer ein oder zwei Schritten „hinterher". Denn um ein entsprechendes Gegenmittel bereitzustellen, müssen die Schadsoftware-Komponenten zunächst erkannt und daraufhin genau identifiziert beziehungsweise analysiert werden. Erste wenn spezielle Eigenheiten des Schädlings bekannt sind, und sich der Verbreitungsweg nachvollziehen lässt, können die entsprechenden Gegenmaßnahmen an die Anti-Viren-Programme ausgerollt werden. zwar bieten die meisten Hersteller von Anti-Schadsoftware auch eine entsprechende Malware-Vorhersage und versuchen zukünftige oder unbekannte Schadsoftware beim „ersten Kontakt" mit ihrer Schutzlösung

Schadsoftware-Kategorien

Seit den Anfängen der IT werden in unregelmäßigen Abständen Schadsoftware-Komponenten und Programme entwickelt, verbreitet und zu unterschiedlichen Zwecken eingesetzt. Folgende Typen werden dabei meist unter dem Begriff „Malware" zusammengefasst:

- Viren,
- Würmer
- Backdoors,
- Bots,
- Trojaner und
- Ransomware.

Bei den Viren handelt es sich dabei um eine der ältesten Schadsoftware-Gattungen: Dabei befällt der Schadcode andere Dateien (meist Anwendungen) und kopiert sich selbst in den Programmcode. Hierbei können sowohl Dateien des Betriebssystems selbst, oder auch Anwendungen und Programme von Drittanbietern befallen werden. Diese kennzeichnet sich dadurch aus, dass der Schädling erst „aktiv" wird, wenn bereits befallene Anwendungen gestartet beziehungsweise eine infizierte Datei geöffnet wird. In den Anfängen der EDV- und IT-Systeme wurden diese Viren meist über Datenträger wie etwa Disketten verbreitet. Neuerer Versionen können (beinahe) alle Arten von Wechselmedien befallen (etwa USB-Sticks) und manchen meist auch nicht vor Online-Speicherplätzen oder Netzlaufwerken halt. Die Analogie zu dem biologischen Virus, quasi einen „Organismus" der fremde Zellen infiziert, wird dabei mehr als deutlich.
Im Gegensatz dazu werden die „Würmer" ohne Aufruf der befallenen Datei aktiv, und verbreiten sich von selbst. Größere Verbreitung erfuhr diese Art

Bild 1. Unterschiedliche Bedrohungen zielen auf unterschiedliche Opfer. Quelle: Microsoft

der Schadsoftware vor allem durch das Internet, hierbei versuchen die „Würmer“ sich in den öffentlichen und privaten Netzwerken zu verbreiten, und ihre Ziele aktiv anzugreifen. Auch hier stand die Biologie Pate, wie bei einer Wurminfektion versuchen die Schädlinge sich aktiv zu verbreiten, und sind auch ohne eine Wirtsdatei in den IT-Systemen „überlebensfähig“.

Bei den Backdoors (oder „Hintertürchen“) handelt es sich um gewollte und geplante Zugangswege zu den Systemen. Diese werden entweder von den jeweiligen Programmierern selbst in Eigenregie in den Quell- beziehungsweise Programmcode eingebettet. Teilweise werden diese Hintertüren auch im Auftrag von Behörden oder Geheimdiensten fest verankert. Andere Firmen wiederum installieren diese Backdoors als Notfallzugang, etwa um Wartungsarbeiten oder Rettungsoperationen bei den betroffenen Anwendungen vornehmen zu können. Solch eine Hintertür kann beispielsweise auch nützlich sein, wenn Fehlkonfigurationen oder Probleme bei der Berechtigung auftreten. So können die Firmen einen Anwendung oder auch ein ganzes Betriebssystem bei schwerwiegenden Fehlern noch „retten“. Problematisch wird es besonders dann, wenn diese Backdoors von Dritten aufgedeckt, und für kriminelle Zwecke ausgenutzt werden.

Bots werden eingesetzt, um fremde Systeme zu übernehmen ohne dass der Besitzer davon Kenntnis erlangt. Die infizierten Systeme werden einem „Botnet“ zusammengefasst. Diese werden in der Regel von einer zentralen Stelle aus angesprochen (Command-and-Control-Server), und „erledigen“ dann eine bestimmte Aufgabe. Meist handelt es sich dabei um DOS-Attacken (Denial Of Service), die Botnet-Betreiber versuchen dabei beispielsweise durch millionenfache Anfragen den Internetzugang eines bestimmten Ziels komplett zu überlasten und lahmzulegen. Auch gegen Webseitenbetreiber und Firmen wird dies oftmals eingesetzt. Hintergründe für solch eine DOS-Attacke können etwa Erpressung sein, („Zahle XYZ Euro oder wir legen deine Webseite lahm!“). Oder Konkurrenten des Unternehmens bezahlen einen Bot-Dienstleister um etwa den unliebsamen Mitbewerber zu blockieren oder zumindest zu stören.

Bei den Trojanischen Pferden wird dem Anwender ein nützlich erscheinendes Tool, ein sinnvolles Programm oder eine wichtige Datei vorgegaukelt, wenn diese daraufhin ausgeführt wird, ruft dies den Versteckten Schadcode auf den Plan. Hierbei sollen den Benutzern im Folgenden bösartige Programme untergeschoben werden, etwa zum Ausspionieren, oder um das System heimlich unter Kontrolle zu bekommen.

Bei der Ransomware handelt es sich um eine Schadsoftware, die den Rechner sperrt, lahmlegt oder die (erreichbaren) Benutzer Daten unbrauchbar macht beziehungsweise verschlüsselt. Dabei werden die Systeme und Daten als „Geisel“ genommen. Meistens wird der Anwender über eine entsprechende Meldung benachrichtigt, auf welche Weise er den Zugang zu den gesperrten Dateien oder Systemen widerherstellen kann. Dies ist in der Regel mit einer Zahlung an den Ransomware-Urheber verbunden. Dabei kommen in der Regel anonymisierte Bezahldienste (wie Ukash, Paysavecard oder Bitcoin-Überweisungen) zum Einsatz.

Bild 2. Der Grund für einen Großteil der Angriffe ist und bleibt die finanzielle Bereicherung. Quelle: Microsoft

Größtenteils harmlos

Zudem sind noch weitere „Kategorien“ vorhanden, meist mit deutlich geringerem Gefährdungspotential wie bei der „echten“ Malware. Dabei ist es nicht das Ziel, Systeme zu kapern, Dateien zu beschädigen oder wie bei Ransomware ein Lösegeld zu verlangen. Eher sollen Klicks auf Webseiten erzeugt, oder Aufrufe von bestimmten Webseiten erreicht werden. Die entsprechenden Programme arbeiten somit eher in einer Art „Graubereich“:

- Browserumleitungen,
- Scareware und
- Adware.

Bild 3. Die Angreifer bleiben meist sehr lange unerkannt im System. Quelle: Microsoft

Diese unerwünschten Software- oder Konfigurationsänderungen zielen beispielsweise darauf ab, die Startseite des Internetbrowser auf eine fragwürdige Seite umzuleiten, etwa um Klicks zu erzeugen, und diese im Anschluss dem jeweiligen Webseitenbetreiber in Rechnung zu stellen. Quasi eine Form von Spam.

Auch hoch im Kurs stehen vermeintliche Virenscanner (Scareware), die nach einem „Scanvorgang" (der nicht stattfindet) dem Anwender eine sehr hohe Anzahl an Viren und Schadsoftware zu präsentieren, dies sich auf dem betroffenen System befinden soll. Das soll zum Kauf dieser (vermeintlich wirksamen) Virenschutzlösung animieren. Oftmals meldet der Scarware-Scanner nach dem Kauf, er habe hunderte oder tausende Viren entfernt, und nun sei wieder alles in Ordnung.

Aber auch unnütze und ungewollte „Helferlein", wie etwa Toolbars, Suchmaschinen, und nutzlose Browsererweiterungen tauschen in regelmäßigen Abständen auf. Hierbei kommen diese Adware-Programme meist „huckepack" mit anderen Anwendungen auf das System. Etwa wenn spezielle Tools von den Anwendern installiert werden, etwa fragwürdige PDF-Konverter, Druckertools oder Anwendungen um spezielle Dateiformate zu öffnen. Unaufmerksame Anwender erlauben dabei die Installation dieser Zusatzsoftware, meist indem die entsprechenden Checkboxen bei der Installation des eigentlichen Tools nicht deaktiviert werden.

Mit den passenden Tools, oder auch mit Windows-Bordmitteln lassen sich diese Softwarekomponenten (meist) relativ einfach wieder entfernen. Hartnäckige Versionen können mit Spezial-Tools wie etwa dem Programm „AdwCleaner" entfernt werden

Mitarbeiter im Fokus

Auch die Mitarbeiter selbst werden gezielt angegriffen. In der Vergangenheit wurde Fälle bekannt, indem Dritte sich telefonisch bei ihren Opfern gemeldet haben, und versuchten an sensible Informationen, wie etwa den Zugangsdaten für ihre Windows-Anmeldung zu kommen. Meist gaben sich diese Personen als „Administratoren" des Unternehmens aus, und wollten eine vermeintliche „Sicherheitsabfrage" oder ähnliches vornehmen. Dazu sollten die Mitarbeiter dann die entsprechenden Informationen mitteilen, angeblich zum Abgleich oder weil das System gerade repariert werden soll. Im Prinzip handelt es sich dabei um eine Adaption des „Enkeltricks", bei dem sich Anrufer als Vertrauensperson Ausgeben, und dann Zugang zu Informationen (oder Geld) fordern. Dies wurde oftmals auch mit dem entsprechenden Überredungsgeschick, sowie dem Aufbau einer Drohkulisse verstärkt. Etwa wenn den Mitarbeitern weisgemacht wurde, sie hätten versehentlich Geschäftsdaten gelöscht, und nun würde ihre Benutzerrechte benötigt um diese widerherzustellen.

Inzwischen fallen die meisten Mitarbeiter nicht mehr auf derartigen Kontaktversuche herein, weder telefonisch noch per E-Mail. Doch die Kreativität der Angreifer bringt immer wieder neue Varianten und Versionen dieses Social-Engineering heraus. Denn aktuell lassen sich meist relativ einfach die Mitarbeiter eines Unternehmens in Erfahrung bringen. Viele Firmen listen die Mitarbeiter samt E-Mail-Adressen direkt auf den entsprechenden Webseiten auf, teilweise mit Bildern und entsprechenden Informationen. Möchten Dritte nun gezielt ein Unternehmen angreifen, genügt es unter Umständen ein oder zwei Mitarbeiter zu identifizieren, die persönliche Informationen beispielsweise in sozialen Netzwerken der Öffentlichkeit preisgeben. Und wenn man die Hobbies, Interessen und damit die „Schwachpunkte" der Mitarbeiter in Erfahrung gebracht hat, sowie womöglich noch das (virtuelle) soziale Umfeld des Opfers beobachtet, kann man passend zugeschnittenes Social-Engineering be-

treiben. Etwa wenn sich das Opfer als leidenschaftlicher Surfer oder Rennradfahrer präsentiert. Hier könnten Dritte genau zugeschnittenen E-Mails von vermeintlichen Freunden oder Bekannten aus der jeweiligen Hobby-Szene (gefälschte E-Mail-Absenderadresse) an das Opfer schicken. Bei solch angepassten Nachrichten ist auch bei „verdächtigen" Emailanhängen (etwa Bilddateien, Office-Dateien oder sogar „getarnten" Anwendungsdateien) eine hohe Öffnungsrate zu erwarten.

Ähnliche Fälle wurden vor kurzer Zeit bekannt, hierbei wurden den Personalabteilungen entsprechend präparierte „Bewerbungen" zugeschickt, die über infizierte Dateianhänge (etwa PDF-Dateien) unter Ausnutzung einer Sicherheitslücke Schadsoftware verteilte. Neu bei dieser Art von Angriff war nun nicht etwa die zugeschnittenen E-Mail, sondern eher die Schiere Masse an E-Mails. Diese waren korrekt formuliert, und bezogen sich auf aktuell ausgeschriebene, offene Stellen. Die „Bewerbungsunterlagen" waren wie von den Unternehmen erwartet, im Dateianhang als PDF zusammengefasst.

Aber auch andere Probleme bei den Mitarbeitern kommen immer wieder zum Tragen. Dabei möchte ein Großteil der Angestellten „nur" seinen Job erledigen. Falls (etwa beim Öffnen einer Datei) Probleme auftreten, versuchen die Mitarbeiter meist das Problem in Eigenregie zu lösen. Daher wird „schnell" eine App installiert, oder im Browser nach einer Online-Konvertierungsmöglichkeit gesucht. Diese Sicherheitslücke „Cloud" ist aktuell eine ständige Bedrohung der Unternehmenssicherheit. Die Cloud nun komplett zu sperren, ist aufgrund der Vernetzung kaum möglich. Denn viele Dienste nutzen das HTTP- oder HTTPS-Protokoll – wie auch der Browser und die entsprechenden Webseiten. Und das Internet komplett sperren ist für beinahe alle Firmen und Unternehmen nicht praktikabel. Somit beschränken sich die meisten Schutzlösungen für Cloud-Applikationen damit, bestimmte (bekannte) Dienste und Anwendungen zu sperren. Doch was machen die Mitarbeiter, wenn man ihnen den Dropbox-Dienst sperrt um weiter Dateien zu teilen? Vermutlich wird auf den nächsten Dienst ausgewichen. Dabei könnte der Einsatz eines unbekannten Speicherdienstes ein noch größeres Risiko darstellen.

Auch ist es möglich, dass sich Personen Zugang zu den Unternehmen verschaffen, um dann direkte Angriffe zu starten. Hier handelt es sich aber eher um Wirtschaftsspionage, und weniger um „normale" kriminelle Aktionen. Je nach Unternehmensgröße sollten die sensiblen Bereiche entsprechend abgesichert werden, denn nicht alle Mitarbeiter sollten Zugang zum Serverraum gestattet werden. Hier helfen physikalische Zugangsbeschränkungen zunächst einmal weiter. Aber auch die Endpoint-Sicherheit ist hier im Auge zu behalten. Schließlich können die unternehmensinternen Clients daraus als „Plattform" für einen effizienten und erfolgreichen Angriff dienen.

Bestimmte andere, lang vorbereitete Attacken dürften dabei allerdings gelingen. Aber auch „spontane Aktionen" sollten die IT-Verantwortlichen bedenken. Etwa wenn sich vermeintlich vertrauenswürdige Mitarbeiter Geschäftsdateien auf USB-Sticks übertragen, und einfach aus dem Haus tragen. Meist sind hier aber nicht eingeschleuste Spione das Problem, sondern normale Mitarbeiter, denen gekündigt wurde. Falls diese eine Kündigung unangemessen empfinden, kann es durchaus vorkommen, dass diese Personen sich „aus Rache" noch alle verfügbaren Dateien kopieren, um diese später weiterzuverwenden. Derartige Möglichkeiten müssen die Verantwortlichen im Blick behalten, und die Benutzerrechte der jeweiligen Mitarbeiter eventuell schon vor dem Kündigungsgespräch entsprechend einschränken.

Dabei gilt es natürlich die Verhältnismäßigkeit abzuwägen. Denn falls es sich um eine ordentliche, betrieblich bedingte Kündigung eines verlässlichen Mitarbeiters handelt, und die Kündigungsfrist etwa drei Monate beträgt, ist es wirtschaftlich eventuell nicht tragbar diesen Mitarbeiter aus der IT „vorsichtshalber" auszusperren. Schließlich soll der Mitarbeiter ja eigentlich noch seine Arbeit beenden können, eine entsprechende Dokumentation für die Übergabe an die Kollegen erarbeiten, um den Abschied möglichst „glatt" über die Bühne zu bekommen.

Auf der anderen Seite wird ein cholerischer, wütender Mitarbeiter – den man aufgrund unterschiedlicher Vergehen bereits in der Vergangenheit abgemahnt hat – gekündigt, sollte man seinen Account eventuell lieber sofort sperren (lassen). Hierbei müssen die Verantwortlichen entsprechen abwägen, und beispielsweise auch einfach auf ihr „Bauchgefühl" hören.

Netzwerk-Monitoring

Ein sehr wichtiger Punkt im IT-Sicherheitsbereich ist sicherlich das Thema „Netzwerküberwachung". Hierbei spielen unter anderem die bereits angesprochenen Firewall-Systeme eine

Rolle. Bestimmte Modelle erlauben es zudem, den übertragenen (TCP/IP-) Datenstrom beziehungsweise den Inhalt der einzelnen Datenpakete zu analysieren. Teilweise ist dies schon in Echtzeit möglich. Dabei können die Netzwerkadministratoren dann entsprechende Dienste blockieren, und beispielsweise Pakete zu bestimmten Diensten verwerfen. Alternativ erhalten die zuständigen Systembetreuer eine entsprechende Warnmeldung, und können dann dieser Sache nachgehen. Auch die Verteilung von internen IP-Adressen sollte bedacht werden. In der Vergangenheit kamen oftmals manuell zugewiesenen IP-Adressen zum Zuge, diese wurden dann in entsprechenden Tabellen (etwa Excel) „verwaltet". Findet sich nun eine IP-Adresse im Netzwerk, die nicht in der Dokumentation auftaucht, könnte dies auf einen unbefugten Zugriff auf das Netzwerk hindeuten.

Derartiges Vorgehen ist inzwischen nicht mehr zeitgemäß. Durch den Einsatz von DHCP-Servern in (beinahe) allen Unternehmen werden die verfügbaren, internen IP-Adressen automatisch beim Anschluss eines Systems verteilt. Trotzdem können hier entsprechende Sicherheitsmechanismen implementiert werden. Denn entsprechende Monitoring-Tools schneiden den Netzwerkverkehr mit, und ermitteln im „normalen" Betrieb die durchschnittlichen Parameter. Falls sich nun bestimmte Abweichungen ergeben, kann dies an die Systembetreuer gemeldet werden, oder auch automatische Reaktionen nach sich ziehen. Beispielsweise wenn ein selten genutzter Drucker plötzlich Daten an eine IP-Adresse im Internet überträgt. Hier liegt dann der Verdacht nahe, dass jemand dieses Gerät „gekapert hat" und das System nun beispielsweise Teil eines Bot-Netzwerks geworden ist.

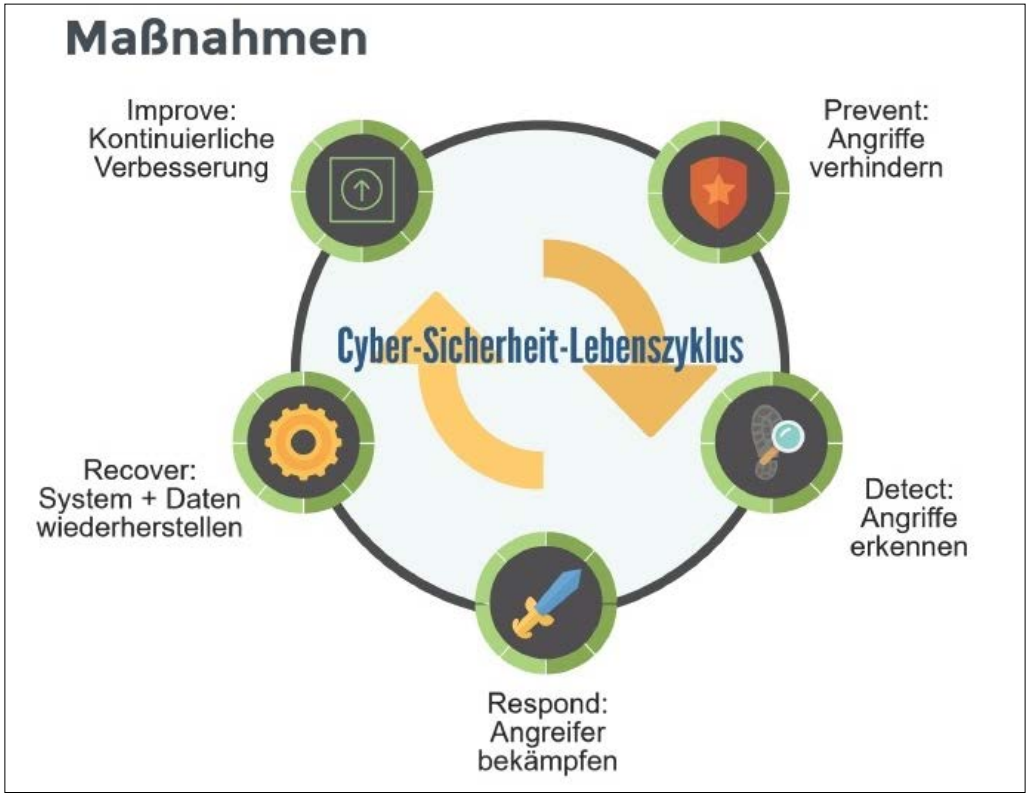

Bild 4. Unterschiedliche Stadien im Kampf gegen Hacker und Malware. Quelle: Microsoft

Aktuell sehr interessant ist es zudem, die Unternehmensnetzwerke auf unerlaubte genutzte Cloud-Dienste abzusichern. Nachdem sich viele dieser Services über das HTTP(S)-Protokoll „unterhalten" benötigen die Systembetreuer an dieser Stelle entsprechende Werkzeuge, um die einzelnen Datenströme entsprechend zu identifizieren. Hier bieten unterschiedliche Dienstleister verschiedenste Möglichkeiten an. Beispielsweise können mit den entsprechenden Hardware-Firewalls bestimmte Dienste und Webseiten geblockt werden, hierbei können die Systembetreuer etwa auf Hardware-Appliances von Checkpoint bauen.

Auch andere Dienstleister und Anbieter haben sich auf derartige Analysen spezialisiert. Hierbei ist beispielsweise das Unternehmen Skyhigh Networks zu nennen. In deren Datenbanken wurden mehr als 20.000 einzelnen Cloud-Dienste erfasst, hier ist besonders wichtig, eine entsprechende Risikoabschätzung vorliegen zu haben. Sprich ist der Cloud-Dienst vertrauenswürdig, zertifiziert und werden die Daten sowohl verschlüsselt übertragen als auch verschlüsselt auf den Anbieter-Servern abgespeichert? Dann kann der Dienst unter Umständen von der Unternehmensleitung genehmigt werden. Bei einem nicht zertifizierten, fragwürdigen Dateidienst fällt die Entscheidung aufgrund fehlender Verschlüsselungsfunktionen dann eher negativ aus.

Auch bei den einzuleitenden Gegenmaßnahmen spielen Netzwerkmonito-

ring-Tools eine bedeutende Rolle. So lassen sich mit den entsprechenden Tools auch unter Umständen die Command-and-Control-Server ermitteln, mit denen etwaige Schadsoftware kommuniziert. Diese werden meist für Bot-Netzwerke eingesetzt, um beispielsweise mit mehreren Millionen infizierter Endgeräte eine Denial-of-Service-Attacke „zu fahren". Um das Unternehmen selbst von derartigen Angriffen abzusichern können sich die Firmen nicht immer auf ihre Internet-Service-Provider verlassen. Denn falls ein KMU (kleine und mittlere Unternehmen) über eine Netzwerkanbindung von 10 GBit/s verfügt, und diese von einer DOS oder DDOS-Attacke komplett belegt wird, kann es für den Service-Provider kaum ersichtlich sein, dass gerade einer seiner Kunden angegriffen wird. Vielleicht bedeutet die komplette Belegung von 10 GBit/s-Kunden-Bandbreite nur einer Schwankung von 0,001 % im gesamten Provider-Netzwerk. Aber auch an dieser Stelle können mit den entsprechenden Appliances Abwehrmaßnahmen vor Ort ergriffen werden.

Angriffe identifizieren

Aber nicht nur die Abwehr, sondern auch die Identifizierung bereits laufender Attacken spielt eine wichtige Rolle. Nach derartigen Aktionen sollten die Verantwortlichen eine entsprechende Analyse der Attacke durchführen, und gegebenenfalls externe Dienstleister in Anspruch nehmen, um das eigenen System – etwa im Rahmen eines Penetrationstests – genauer unter die Lupe zu nehmen.

Laut einigen Studien benötigen potentielle Angreifer nur relativ geringe Zeitspannen, um Systeme zu infizieren oder zu infiltrieren. Denn falls diese Aktionen entsprechend geplant werden, bekommen diese „schnell einen Fuß in die Tür". Dabei müssen noch gar keine Administratorrechte für die Angreifer zur Verfügung stehen, meist gelingt im ersten Schritt der Zugriff auf eher unbedeutende Systeme. Etwa einem Windows-Clients eines „normalen" Mitarbeiters mit eingeschränkten Benutzerrechten. In weiteren Schritten erweitern die Angreifer ihren Zugriff aus den Systemen, und versuchen immer weiter vorzudringen. Dabei bedienen sie sich ähnlicher Werkzeuge und Tools wie auch die Administratoren für ihre alltägliche Arbeit einsetzen. Beispielsweise Fernwartungs-Tool, Netzwerkanalyseprogramme oder Bordmittel wie die Windows-Kommandozeile (CMD) oder auch die Windows Powershell (PS).

Wenn man sich allerdings die durchschnittliche Zeit genauer betrachtet, die Unbefugte in den IT-Systemen der Unternehmen verbringen, eher die Attacke entdeckt wird, staunen die meisten Sicherheitsbeauftragten: Durchschnittlich verbringen die „Hacker" 140 Tage bis der Einbruch entdeckt wird. Zusätzlich benötigen die Systembetreuer nochmals etwa zwei Monate, um die Sicherheitslücken zu schließen und den Angriff komplett abzuwehren.

Dabei haben die Angreifer es nicht immer nur auf den Datenbestand des infiltrierten Unternehmens abgesehen, sondern nutzen das Netzwerk auch als „Sprungbrett" um beispielsweise Kunden oder Partner des angegriffenen Unternehmens ebenfalls zu infiltrieren.

Daher sollten die Systembetreuer unsichere Administrator-Werkzeuge deaktivieren und etwa per Gruppenrichtlinie oder durch entsprechende Firewall-einstellungen unbrauchbar machen. Zum Management der Systeme sollten die Administratoren dann möglichst nur wenige Werkzeuge nutzen. Ein guter Kandidat hierbei ist etwa die Powershell. Denn mit diesem Bordmittel lassen sich sehr viele unterschiedliche Verwaltungsfunktionen abdecken. Zudem können die Systembetreuer entsprechende Logging-Funktionen einsetzen, um sämtliche PS-Aktionen von allen Systemen im Netzwerk entsprechend zu protokollieren. Diese Log-Dateien könnten auch beispielsweise auf mehrere Server im Unternehmen verteilt werden. Falls nun die Angreifer versuchen, ihre Fußspuren auf Server-A zu verwischen, werden diese PS-Befehle an anderer Stelle (Server-B und Server-C) protokolliert.

Aktive Gegenmaßnahmen einleiten

Falls ein Angriff entdeckt wird, sollten die Systembetreuer sofort die Verantwortlichen inm Unternehmen persönlich benachrichtigen. Schließlich könnten die Hacker eventuell auch die Nachrichten in der Unternehmensinternen (E-Mail-) Kommunikation überwachen, um festzustellen ob ihre Attacke „aufgeflogen" ist. Danach sollte die Entscheidung getroffen werden, ob sofort entsprechende Abwehrmaßnamen getroffen werden sollen, etwa das Bereinigen von befallenen Clients oder Servern, das Einspielen von Bare-Metal-Backups oder eine aktive Blockierung der IP-Adressen, von denen aus Zugriffe auf das interne Netzwerk festgestellt wurde. Alternativ könnten die Systemverantwortlichen auch versuchen die

Quelle des Angriffs genauer zu identifizieren, und den Angreifer weiter in dem Glauben lassen, er wäre weiterhin unentdeckt.

Falls das Know-How der internen IT-Abteilung nicht für eine erfolgreiche Abwehrschlacht ausreicht, sollten sich die Systembetreuer auch an entsprechende Dienstleister wenden. Viele größere Unternehmen (etwa Dell) bieten inzwischen eigene IT-Security-Sicherheitsteams an, die auch bei derartigen Problemen mit Rat und Tat zur Seite stehen. Unter Umständen sollte an dieser Stelle auch eine Anzeige gegen Unbekannt, und eine forensische Analyse sämtlicher Angriffsprogramme, Infektionswege und Kommunikationskanäle der Angreifer vorgenommen werden.

Im Schlimmsten Fall können die Systembetreiber immer noch „den Stecker ziehen", und das System temporär vom Internet trennen, sämtliche Arbeitsstationen und Server Scannen, bereinigen und danach das System wieder online bringen

Detailliertes Rechtemanagement

Einen wirksamen Schutzschild gegen unterschiedliche Angriffsszenarien bietet ein ausgefeiltes Rechtemanagement. Auch die Systembetreuer sollten immer nur mit den gerade benötigten Berechtigungen „arbeiten" die für die momentan anfallenden Aufgaben benötigt werden. Falls etwa nur eine Datenbank gewartet werden soll, benötigt der Systembetreuer keine Domänen-Administratorberechtigung und diese Aufgabe erfolgreich abzuschließen. Ebenso sollte mit den Berechtigungen für die Mitarbeiter verfahren werden. Das Credo: „So viel wie nötig, so wenig wie möglich" ist dabei anzuwenden.

Auch erweiterte Authentifizierungs-Möglichkeiten sollten dabei in Betracht gezogen werden. Etwa Multi-Faktor-Authentifizierung, Zertifikate auf den entsprechenden Systemen, um sicherzustellen das die Kommunikationsgegenstelle auch wirklich ein vertrauenswürdiges System darstellt, und nicht etwa ein „Man-in-the-middle-Angriff" stattfindet.

Sinnvoll ist an dieser Stelle auch etwa, wenn die Benutzer-Accounts nur Zeitlich begrenzt angelegt werden. Dies ist zwar mit den Windows-Bordmitteln nicht möglich, kann aber über entsprechende Tools von Drittanbietern (etwa Quest) realisiert werden.

Auch die Backup-Strategie muss hier mit eingebunden werden. Etwa falls die Systembetreuer auf den Clients zusätzliche Backup-Accounts einrichten, und diese Anmeldedaten für den Zugriff auf ein Netzlaufwerk einsetzen. Nur dieser Backup-Account bekommt etwa Schreibrechte auf den Backup-Netzlaufwerk, und alle anderen User nur Leserechte. Falls sich nun ein Ransomware-Trojaner auf einem der Mitarbeitersysteme einnistet, so wird dieser als „normaler" Benutzer ausgeführt, und erhält auch nur Lesezugriff auf die verbundenen Backup-Speicherorte. Auf diese Weise können die Systembetreuer schnell eine Wiederherstellung (etwa per USB-Boot-Stick) starten, und das System wieder in einen sicheren Zustand versetzen.

Proaktive Ansätze helfen

Anstatt erst zu reagierten, wenn die Schadsoftware oder der Hacker versucht Zugriff auf die Systeme zu erlangen, können die Unternehmen auch den „Spiess umdrehen, und ihre Systeme auf diesen Ernstfall entsprechend vorbereiten. Hierbei ist es etwa interessant, wenn bestimmte Werkzeuge und Tools eingesetzt werden, die sämtliche Zugriffe erst einmal in einem abgeschlossenen Bereich umleiten". Etwa wenn virtuelle Maschinen (VMs) genutzt werden, oder Schreibzugriffe in eine RAM-Disk umgeleitet werden. An dieser Stelle sollte auch noch hervorgehoben werden, dass Sandboxing" eine sehr hohe Resistenz gegen Angriffe von außen bietet. Dabei werden Anwendungen, Programme, Dienste und Threads vom Betriebssystem oder vom Benutzerkonto „isoliert". Im Hintergrund nutzen diese Anbieter meist ebenfalls die ausgefeilte Windows-Berechtigungs-Hierarchie. Bei der Lösung von Avecto (Defendpoint) etwa können gefahrlos infizierte Dateianhänge mit versteckter Ransomware geöffnet werden.

Denn im Hintergrund wird beim Windows-Start quasi ein „frischer" Benutzer-Account angelegt, und sämtliche geöffnete Anwendungen (Office, E-Mail, Webbrowser, Fotoprogramm oder ähnliches) nur mit diesen Berechtigungen ausgeführt. Ein Ransomware-Trojaner kann in diesem Fall auch nur die Daten des temporären Benutzers verschlüsseln und unbrauchbar machen. Bereits nach einem Neustart oder einer Neuanmeldung werden diese Daten sowie die Viren oder auch installierte Anwendungen automatisch gelöscht. Der Vorteil dabei liegt auf der Hand. Selbst noch unbekannte Malware oder sonsti-

ge unerwünschten Programme werden zuverlässig neutralisiert.

Netzwerkunterteilung

Ebenfalls ein interessanter Ansatz um Schadsoftware wie Erpressungstrojaner abzuwehren ist es, das interne Netzwerk entsprechend zu unterteilen, Etwa in ein oder zwei „sichere" Zonen (Server im Serverraum), eine Zone mit mittlerer Gefährdung („normale" Clients in den Abteilungen) und beispielsweise eine „Hochrisiko-Zone" (mobile Endgeräte von Kunden, Mitarbeitern und Gästen im Unternehmens-WLAN) zu unterteilen. Aus aktuellem Anlass sollten die Firmen auch in Betracht ziehen, bestimmte Abteilungen die mit unter Umständen unbekannten kommunizieren (Werbeabteilung, Personalabteilung) ebenfalls entsprechend abzuschotten. „Sollte sich nun ein Erpressungstrojaner breitmachen", so wird dieser das entsprechende Subnetz (kaum) verlassen können. Damit bleibt eine Infektion mit Schadsoftware auf einem kleineren Raum begrenzt, und sich somit leichter unter Kontrolle bringen.

Kreative Angreifer, stark wachsende Malware-Gefahren und immer ausgefeilter Social-Engineering erhöhen die Gefahr für die IT in den Unternehmen von Tag zu Tag. Die Angreifer kombinieren dabei bekannte Methoden und Programme immer wieder neu, und passen ihre Strategien immer wieder an. Das macht es für die Sicherheitsbeauftragen in den Unternehmen, für die Systembetreuer und Administratoren und auch für die Mitarbeiter immer schwieriger, für die Sicherheit der Unternehmens-IT zu sorgen. Doch nur wenn alle Teile des Unternehmens und alle Mitarbeiter entsprechend sensibilisiert werden, können Angriffe abgewehrt, entdeckt oder bekämpft werden. Hierbei sollten sich die Sicherheitsbeauftragten von den Hackern eine Scheibe abschneiden, und ebenfalls mehrerer Methoden, Programme und Abwehrstrategien kombinieren. Etwa wenn aktuellen Betriebssysteme, tägliche Updates, Virenschutzprogramme, Firewalls, Sandbox-Systeme und unterschiedliche Netzwerke in den Unternehmen eingesetzt werden, kann der Aufwand für einen erfolgreichen Angriff massiv erhöht werden. Dies kann unter Umständen bereits ausreichen, dass sich die Hacker einem anderen, lohnenderen Ziel zuwenden. Das löst zwar nicht das Problem an sich, aber verlagert dies entsprechend. Getreu nach dem Motto „Heiliger Florian, verschone unser Haus, zünd andere an!"

Florian Huttenloher

NT4ADMINS MAGAZIN

NT4ADMINS ist eine Publikation der MBmedien Publishing GmbH,
Europark Fichtenhain A 13a,
47807 Krefeld
Telefon: 02151 / 5192-0,
Telefax: 02151 / 5192-999
Email: info@mbmedienpublishing.de
Website: www.mbmedien.de/unternehmen.html

Vertretungsberechtigter Geschäftsführer:
Stefanie Ahl, Jannis Moutafis,
Rainer Huttenloher
Handelsregistereintrag:
Amtsgericht Krefeld HRB 13221
Steuer-Nr. 117/5824/2990
Umsatzsteuer ID-Nummer: DE 293969983
Verantwortlich im Sinne § 5 TMG bzw. § 55 RStV: Stefanie Ahl, Jannis Moutafis, Rainer Huttenloher
Büro München: Landsberger Straße 396, 81241 München
Chefredakteur: Rainer Huttenloher (rhh) (v.i.S.MdStV.)
Mail: rhuttenloher@mbpublishing.de
Landsberger Straße 396, 81241 München
Verantwortlich für den redaktionellen Teil

Redaktion:
Rainer Huttenloher (rhh),
Florian Huttenloher (fah)
Ständige freie Mitarbeiter zu erreichen unter der Anschrift der Redaktion bzw. per Mail unter service@nt4admins.de

Layout:
David Popp, POPP MEDIEN, Augsburg

Erscheinungsweise:
Monatlich: (Doppelausgaben zum Juli/August und Dezember/Januar)

Bezugspreise:
Abonnements nur über Website:
www.nt4admins.de/registrierenabo/aboauswahl.html

WaaS – Windows 10 im Unternehmenseinsatz

Spätestens seit dem Release von Server 2016 geht es in den Unternehmen aufwärts mit Windows 10. Denn nun steht den Firmen sowohl bei dem Clients, als auch bei den Serversystemen die gleiche Windows-Kernel-Basis zur Verfügung. In der Vergangenheit hatte sich diese Kombination als optimale Windows-Lösung herauskristallisiert, und dies bestätigt sich wieder bei Windows 10 und Server 2016. Zusätzlich wird Windows 10 permanent weiterentwickelt, Microsoft liefert mit den entsprechenden „großen" Updates regelmäßig jede Menge Funktionen nach. Dies ist aber nicht in jedem Fall erwünscht, dies hat Microsoft erkannt, und ermöglicht die Verzögerung dieser Funktions-Updates unabhängig von sicherheitskritischen Patches und Hotfixes.

Windows 10 wurde vielfach als „letztes" Windows bezeichnet. Dies ist der Tatsache geschuldet, dass Microsoft weiterer Funktionen über entsprechende Service-Packs und Updates nachrüstet. Windows 10 soll auf diese Weise permanent weiterentwickelt werden. Dies wird unter dem Begriff WaaS (Windows as a Service) zusammengefasst, analog zum „Software as a Service" (SaaS). Der Hintergrund: das Betriebssystem als Software-Kernkomponente soll aus dem Hauptgeschäft langsam herausfallen. In Zukunft möchte Microsoft sein Geld eher als Software-Dienstleister und Cloud-Provider verdienen, und weniger mit dem Verkauf neuer Betriebssystemgenerationen. Inzwischen läuft Windows 10 schon auf (beinahe) jedem aktuellen System. Wenn sich Anwender entscheiden einen neuen Windows-PC oder ein Laptop kaufen, ist dabei in der Regel Windows 10 voristalliert. Auch im geschäftlichen Umfeld kommt die aktuelle Client-Version bereits in einer großen Anzahl zum Einsatz. Einzig im Mobilbereich (etwa Tablets und Smartphones) haben die Mitbewerber (etwa Apple mit iOS oder Google mit Android) die „Nase" vorn.

Migration nötig?

Trotz der steigenden Verbreitung von Windows 10 setzen viele Unternehmen im Moment noch auf ältere Client-Betriebssysteme. Relativ verbreitet sind beispielsweise Windows 7 oder Windows 8.1, während Windows 8 oder Vista inzwischen kaum noch anzutreffen sind. Teilweise werden allerdings noch ältere Systeme eingesetzt, bei denen der Microsoft-Support längst abgelaufen ist. Hier ist immer noch Windows XP zu nennen, sogar Versionen von Windows 2000 oder Windows 98 sind noch vereinzelt im Einsatz. Diese Systeme werden meist offline eingesetzt, in der Regel werden damit noch bestimmte Steuerungsfunktionen übernommen. Etwa wenn eine inzwischen veraltete Software weiterhin eingesetzt werden soll. Bei diesen Systemen ist es meist nicht möglich, auf eine aktuelle Version umzustellen, etwa wenn der Programmierer der „Speziallösung" schon längst nicht mehr greifbar ist. Oder wenn seit Jahren „alles super läuft", und die Verantwortlichen das System so lange nützen möchten, bis es sprichwörtlich auseinanderfällt.

Somit lässt sich die Frage, ob unbedingt auf ein aktuelles Client-betriebssystem umgestellt werden sollte nicht einheitlich antworten. Bestimmte Argumente sprechen für den Umstieg, einige dagegen. Zudem ist es generell wichtig, immer auf dem aktuellsten Update-Stand zu bleiben. Falls nun für das eingesetzte OS keine Windows-Updates mehr herausgebracht werden (etwa bei Windows XP), so sollten diese Systeme keinesfalls mehr Kontakt mit dem Internet bekommen – zu hoch ist dabei das Infektionsrisiko. Spätestens dann sollten die Systembetreuer und IT-Verantwortliche Aktualisierungen starten.

Im Großen und Ganzen bieten die aktuellen Client-Versionen, wie etwa Windows 10 auch die höchste Widerstandsfähigkeit, etwa was Schadsoftware-Angriffe angeht. Auf der anderen Seite könnte man ins Feld führen, dass es deutlich wahrscheinlicher ist, dass sich unentdeckte Sicherheitslücken in den aktuellsten Versionen befinden, als in einem älteren, und dadurch in der Praxis bewährten System wie etwa Windows 7.

Aus finanzieller Sicht befinden sich die Systemverantwortlichen ebenfalls in der „Zwickmühle". Zum einen wird für aktuelle Betriebssysteme meistens auch aktuelle Hardware benötigt, was wieder-

um weitere Investitionen nach sich zieht. Zum anderen kann durch die Umstellung auf eine aktuelle Betriebssystemgeneration unter Umständen einiges an laufenden Kosten eingespart werden. Dies ist etwa der Fall wenn in den Unternehmen bisher ein Mix aus unterschiedlichen Systemen betreiben wird. Beispielsweise wenn noch ältere Windows-7- sowie Windows-8.1-Systeme in den Abteilungen vorhanden sind, und inzwischen weitere Windows-10-Geräte (etwa Notebooks, Tablets oder Smartphones) hinzugekommen sind. Nun dürfen sich die Administratoren mit Serviceanfrage zu drei unterschiedlichen Betriebssystemen „herumschlagen". Vereinfacht man dies nun, und stellt komplett auf Windows 10 um, ergeben sich in der Regel deutliche Einsparmöglichkeiten, das Admin-Personal kann sich so auf ein System konzentrieren.

Im selben Maße sollte an die Server-Infrastruktur gedacht werden. Denn was für die Clients gilt, trifft oftmals auch auf die Serversysteme zu. Dabei ist es (meist) sinnvoll, bei den Clients sowie den Servern auf eine gemeinsame Windows-Kernel-Basis zu bauen. Sprich Windows Server 2012 R2 in Verbindung mit Windows 8.1 oder Windows Server 2016 in Kombination mit Windows 10. Dies wird vor allem beim Einsatz von Gruppenrichtlinien deutlich, diese spielen bei identischem Funktionsumfang (meist) besser zusammen.

Insgesamt lässt sich feststellen: Früher oder später sollten die Systeme auf die aktuellste Version gebracht werden, die Frage ist eher, wann der günstigste Zeitpunkt gekommen ist. Dies müssen die Firmen selbst festlegen, und unterschiedliche Argumente gegeneinander abwägen, denn eine pauschale Empfehlung lässt sich dabei kaum treffen.

Sicherheits-Features

Grundsätzlich sind aktuelle Systeme mit den neuesten Pach-Level sicherer als ältere Betriebssysteme mit veralteten Patch-Stand. Zwar können unbekannte Sicherheitslücken in allen Systemen vorhanden sein (Exploits). Generell gehen die Systembetreuer sicherer mit diesen gefahren um, wenn aktuelle Server- und Client-Betriebssysteme mit aktuellen Updates und Patches eingesetzt werden. Zusätzlich sollen unter Windows 10 weitere Funktionalitäten die Sicherheit im Vergleich zu den Vorgängerversionen erhöhen:

- Das Bordmittel „Windows Defender" wurde verbessert, in der aktuellen „Creators Update" sollen dank der ATP (Advanced Thread Protection) nun auch etwa der Hauptspeicher auf Manipulationen hin überwacht werden.
- Die Windows-Firewall soll als „Torwächter" Hackern und Malware das Leben schwermachen.
- Funktionen wie die Benutzerkontensteuerung oder der SmartScreen-Filter für Apps erhöhen die Sicherheit zusätzlich.
- Im Vergleich zum Internet Explorer bietet Edge einen höheren Funktionsumfang und eine verbesserte Sicherheit.
- Das Management kann inzwischen komplett mit den entsprechenden Servertools vorgenommen werden.
- Zudem lassen sich die Windows-Clients und Windows-Server durch die Bank mit Hilfe der Windows Powershell verwalten, auf diese Weise liefert Microsoft „das Kommandozeilen und Skripting-Werkzeug" gleich als Bordmittel mit.

Aktuelle Windows 10-Versionen nach Wartungsoption

Wartungsoption	Version	OS build	Verfügbarkeitsdatum	Letztes Revisionsdatum	
Current Branch (CB)	1607	14393.576	8/2/2016	12/13/2016	*Microsoft empfiehlt*
Current Branch (CB)	1511	10586.713	11/12/2015	12/13/2016	
Current Branch (CB)	1507 (RTM)	10240.17202	7/29/2015	12/13/2016	
Current Branch for Business (CBB)	1607	14393.576	11/29/2016	12/13/2016	
Current Branch for Business (CBB)	1511	10586.713	4/8/2016	12/13/2016	
Current Branch for Business (CBB)	1507 (RTM)	10240.17202	7/29/2015	12/13/2016	
Long-Term Servicing Branch (LTSB)	1607	14393.576	8/2/2016	12/13/2016	
Long-Term Servicing Branch (LTSB)	1507 (RTM)	10240.17202	7/29/2015	12/13/2016	

Bild 1. Eine Übersicht der aktuellen Windows-10-Builds nach den gewählten Wartungsoptionen. Quelle: Microsoft

- Einen Gesamtüberblick der Sicherheitsfunktionen liefert der „Windows Security Manager“ dabei ist es zudem möglich, das SaaS-Angebot „Office 365“ im Zusammenspiel mit der „Office 365 Advanced Thread Protection“ zu überwachen.

In Verbindung mit weiteren Anti-Virenschutzlösungen, einem durchdachten Rechtemanagement (mit oder ohne Active Directory möglich), sowie entsprechenden Backup-Lösungen kann eine hohe Resistenz gegenüber Schadsoftware-Infektionen aufgebaut werden. Falls dies noch nicht ausreicht, installieren die Administratoren entsprechende Sandbox-Systeme, unterteilen das Unternehmensnetzwerk in unterschiedliche Subnetze und mildern die Folgen von Malware durch entsprechende Firewall-Systeme ab.

Management-Tools

Insgesamt bieten sich bei Windows 10 unterschiedliche Wege und Methoden an, um die Systeme zu verwalten, Änderungen vorzunehmen, Gruppenrichtlinien anzuwenden oder Mobilgeräte mit einzubinden. Während für die Server-Varianten etwa die RSAT-Tools (Remote Server Administration Tools) bereitstehen, lassen sich die Windows-10-Clients beispielsweise über den Mobile Device Manager verwalten. Auch die klassischen Ansätze, etwa über GPO (Gruppenrichtlinien-Objekte) lassen sich die Clients wie gewohnt ansprechen und konfigurieren.

Wartungstool	Können Updates zurückgestellt werden?	Möglichkeit zum Genehmigen von Updates	Peer-to-Peer-Option	Weitere Funktionen
Windows Update	Ja (manuell)	Nein	Übermittlungsoptimierung	Keine
Windows Update for Business	Ja	Nein	Übermittlungsoptimierung	Andere Gruppenrichtlinienobjekte
WSUS	Ja	Ja	BranchCache oder Übermittlungsoptimierung	Upstream-/Downstream-Skalierbarkeit des Servers
Configuration Manager	Ja	Ja	BranchCache, Clientpeercache	Verteilungspunkte, mehrere Bereitstellungsoptionen

Bild 2. Die Windows-Updates lassen sich über unterschuiedliche Wege bereitstellen.

Quelle: Microsoft

Windows as a Service

Für die Unternehmen sind insgesamt drei „Service-Pläne“ verfügbar. Damit möchte Microsoft den Firmen genug Flexibilität bieten. Unter anderem unterscheiden sich diese Pläne durch die mögliche Verzögerung von Updates und Aktualisierungen. Denn oftmals möchten die Systembetreuer erst dann bestimmte Updates, die den Funktionsumfang verändern, aufspielen, wenn diese ausreichend getestet wurden. Hierbei sind nun nicht unbedingt sicherheitsrelevante Hotfixes und Patches gemeint, diese sollten in der Regel besser nicht „verschoben“ werden. Um diese Möglichkeiten zu bieten, stehen die folgenden Pläne zur Verfügung:

- Current Branch (CB),
- Current Branch for Business (CBB),
- Long Term Servicing Branch (LTSB).

Beim CB-Modell werden die Updates verfügbar, wenn Microsoft diese freigibt. In älteren Versionen von Windows 10 (Build 1511 oder früher) standen nur wenige Möglichkeiten zur Verfügung, um im CB-Plan einzelnen Updates zu verzögern. Ab Version 1607 wurde dies angepasst, und inzwischen lassen sich bestimmte Features, Funktionen und Updates um bis zu 180 Tage verzögern. Dieser Service-Plan ist für Anwender und Systembetreuer geeignet, die „frische“ hinzugefügte Features im Zuge der Windows-Updates einsetzen möchten, etwa um immer auf dem neuesten Stand zu bleiben, oder um diese aktuellen Features zu testen.

Wenn Microsoft ein neues Feature per Windows-Update zur Verfügung stellt, wird dies für den CB-Serviceplan markiert, und (zunächst) umgehend an alle Systeme mit CB-Plan ausgerollt. Falls in den Unternehmen WSUS-Server diese Verteilung übernehmen, den Microsoft System Center Configuration Manager oder Windows Update für Business, so können diese Features entsprechend verzögert werden. Allerdings sollten die Systembetreuer dabei im Hinterkopf behalten, dass einzelne Builds von Windows 10 aufeinander aufbauen. So ist es zwingend notwendig, die „älteren“ Funktionen und Updates hinzuzufügen, bevor auf die aktuellste Version upgedatet werden kann.

Bei dem Service-Plan CBB dagegen werden nicht primär Testsysteme mit Updates „versorgt“. CBB eignet sich durch seine „konservative“ Update-Einstellung eher für den breitgefächerten Rollout und die komplette Update-Versorgung von Produktivsys-

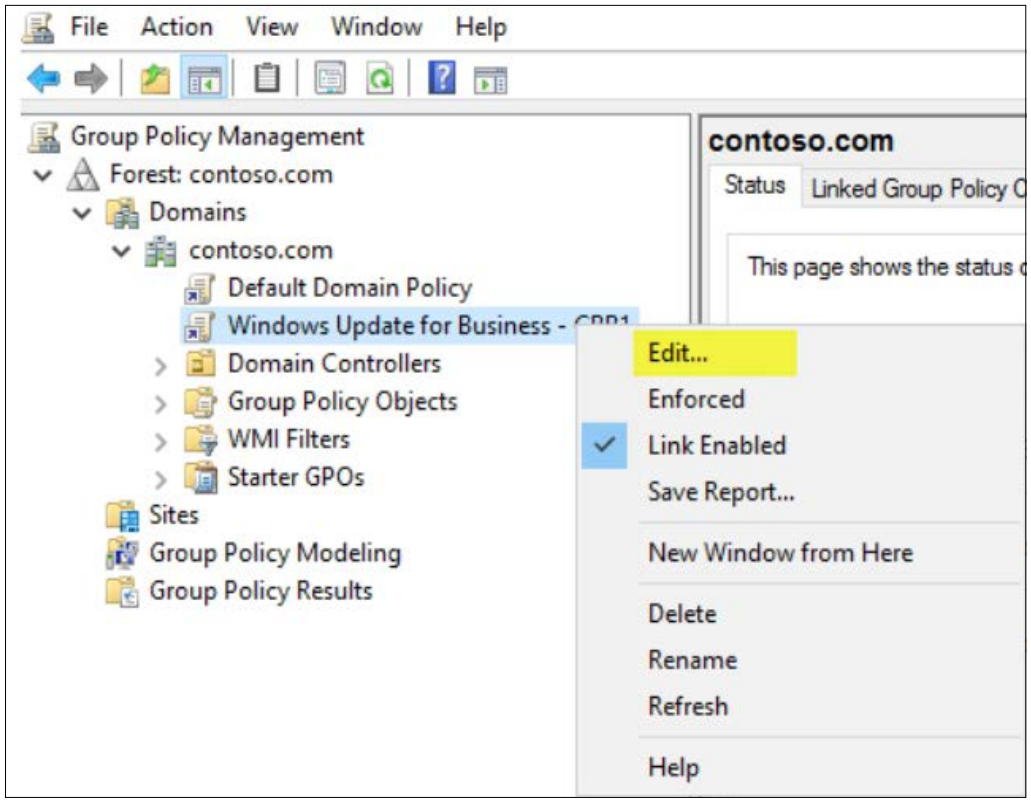

Bild 3. Mit dem „Windows Update for Business" wird die Zustellung der Updates über Gruppenrichtlinien gesteuert – ideal für kleine und mittlere Unternehmen ohne WSUS-Server. Quelle: Microsoft

temen. Im Prinzip erhalten alle CBB-Systeme die gleichen Updates wie die Versionen mit CB. Allerdings werden diese Features im Vergleich zu CB deutlich verzögert. Generell werden Funktionsänderungen um vier Monate verzögert – dies ist etwa die durchschnittliche Zeitspanne, in denen Hardware-Hersteller, Software-Firmen und Systemhäuser benötigen, die „frischen" Funktionen auf „Herz und Nieren" zu prüfen. Insgesamt werden mit CBB zwei unterschiedliche „Windows-Builds" unterstützt, um im Unternehmen für eine höhere Flexibilität im Gegensatz zu CB zu sorgen (bei CB wird immer nur eine vorangegangene Build-Version unterstützt). Jedes Feature-Update-Release befindet sich dabei mindestens 180 Tage auf der Kompatibilitäts-Liste.

„Never touch a running system!" – Bei bestimmten Systemen gilt dieses Credo ganz besonders. Etwa wenn Clients zur Steuerung von weiteren Maschinen, Systemen, Druckern, Plottern, Fräsmaschinen, oder ähnlichen Zwecken eingesetzt werden. Denn hier gilt es oftmals, nur eine einzige Anwendung oder einen einzigen Dienst bereitzustellen, wie etwa bei Videotheken-PCs oder Geldautomaten. Weitere Funktionen sind dabei nicht gewünscht, viel wichtiger ist es dagegen, dass dies zu zuverlässig wie möglich mit sehr geringen Ausfallzeiten geschieht. Für eben solche Systeme bietet sich bei Windows-10 im Unternehmenseinsatz der LTSB an. Somit werden die Feature-Updates übersprungen, und einzig sicherheitsrelevante Hotfixes und Patches aufgespielt. Microsoft offeriert dagegen alle zwei bis drei Jahre neue LTSB-Versionen, dabei können sich die Unternehmen dann entscheiden, ob diese neuere Build eingesetzt werden soll, oder ob das System weiter in der „älteren" Version betrieben werden soll. Microsoft stellt dabei Supportzeiten von zehn oder mehr Jahren für einzelne LTSB-Versionen in Aussicht.

Zusammenfassung

Windows 10 ist inzwischen eine feste Größe in den Unternehmen, dank der kontinuierlichen Weiterentwicklung dürfte das aktuelle Client-Betriebssystem in Zukunft weiter an Attraktivität gewinnen. Rüstet Microsoft in regelmäßigen Abständen – wie dem Creators Update – frische Features nach. Für die Unternehmen ist es dabei meistens interessant, wenn die Sicherheit erhöht wird, das Handling vereinfacht, oder die Servicezeiten, etwa aufgrund verbesserter Management-Funktionen, verringert werden können. Aber auch bei bestimmten Systemen, die keine (Funktions-) Updates benötigen, hat Microsoft mit dem Service-Plan LTSB einiges in petto. Weitere Informationen finden die Systembetreuer in den entsprechenden Technet-Seiten.

Damit können sich die Anbieter von Steuerungscomputern, Geldautomaten oder Videotheken-Systemen sicherstellen, dass „ihr" System auch in zehn Jahren noch genauso stabil und ohne Veränderung läuft, wie mit der aktuellen Version. Mit einem Unterschied: Sicherheitskritische Updates wurden im Laufe der Zeit immer eingespielt, das System ist Patch-mäßig somit immer auf dem neuesten Stand. **Florian Huttenloher**