SYSTEM IN GEFAHR

Malware-Infektionen erkennen und verhindern

solarwinds msp

INHALT

Zu den anspruchsvollen Aufgaben der IT gehört es, Computernetzwerke vor Unbefugten zu schützen. Es gibt viele Angriffsmethoden mit unterschiedlichem Gefahrenpotenzial. Mit Überreaktionen oder dem falschen technischen Ansatz kann man enorme Kosten verursachen und es den Cyberkriminellen unter Umständen sogar noch leichter machen.

In diesem E-Book werden typische Internetbedrohungen geschildert, denen ein Netzwerk heutzutage ausgesetzt ist, und jeweils angemessene Schutzstrategien beschrieben.

Der Leitfaden versteht sich als Einstiegslektüre für den Aufbau eines grundlegenden Schutz- und Abwehrkonzepts. Als IT-Experte müssen Sie sich zwei Dinge bewusst machen: Erstens, Internetkriminalität erzeugt ein beträchtliches Geschäftsrisiko. Zweitens, bis dato ist leider kein Kraut dagegen gewachsen. Auch wenn mancher Anbieter das gerne behauptet: Die eine Technik, mit der Sie sich alles vom Leib halten können, gibt es nicht.

Jede erdenkliche Cybergefahr, Malware oder Sicherheitslücke dieser Welt wurde schon durch die hochemotionale Medienmaschine gedreht – ohne Rücksicht auf die tatsächliche Faktenlage. Dabei sind die probaten Mittel gegen unbekannte und bekannte Gefahren im Großen und Ganzen unverändert die folgenden: Betriebssystem und Anwendungen aktuell halten und regelmäßig patchen, Administratorrechte nicht zu lax handhaben und Abwehrsysteme gegen Malware verwenden. Grundlage für diese Empfehlungen sind die von vielen Regierungs- und Sicherheitsorganisationen weltweit seit Jahren durchgeführten Datenanalysen.

Letztlich gilt: „Offense informs defense“ – jeder Angriff liefert aufschlussreiche Daten für seine künftige Abwehr. Was heißt das? IT-Verantwortliche müssen die unter ihrer Obhut stehenden Netzwerke durch die Brille der Angreifer sehen lernen. Das soll keine Aufforderung zur Entfaltung eigener krimineller Energien sein. Aber wer sich zum Beispiel ein Cyberabwehrlabor einrichtet und ein paar kostenlose Tools zur Schwachstellensondierung nutzt, wird peu à peu geschickter darin, den Eindringlingen das Handwerk zu legen.

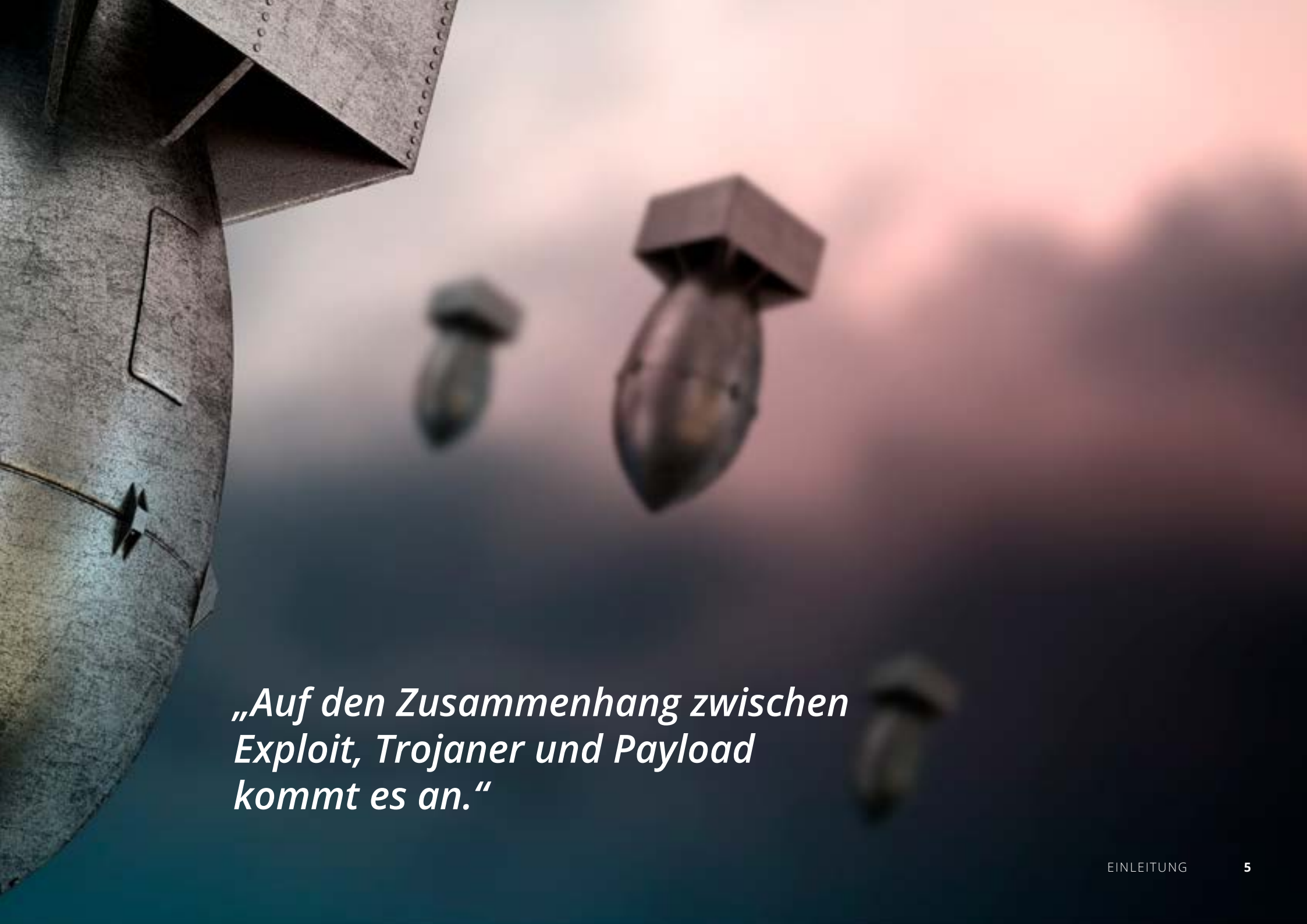
Denken Sie daran: Als IT-Fachmann oder -frau sind Sie ganz oder teilweise für den Datenschutz, die Integrität und die Verfügbarkeit der Systeme zuständig, die man Ihnen anvertraut hat. Machen Sie den Schurken da draußen also das Leben schwer. Sorgen Sie dafür, dass sie sich an einem eisernen Schutzkonzept aus Erkennung, Prävention und Forensik die Zähne ausbeißen.

EINFÜHRUNG

Bei Diskussionen über Netzwerksicherheit geht es über kurz oder lang um die Frage, was Antiviren-Software gegen Malware auszurichten vermag. Speziell das Thema Ransomware brennt allen Sicherheitsspezialisten auf den Nägeln. Qualifiziert kann man sich zu dieser Frage nur äußern, wenn man die Zusammenhänge zwischen Exploits, Trojanern und Payloads versteht.

Auf Seite 7 sehen Sie ein fünfgliedriges Schema, das sich an die von Lockheed Martin entwickelte Cyber Kill Chain® anlehnt und den Verlauf eines Netzwerkübergriffs von der Ausnutzung eines Sicherheitsschlupflochs bis hin zur Erreichung des eigentlichen Ziels beschreibt.[1] Dabei durchläuft ein Angriff von der Verteilung oder Zustellung schädlicher Inhalte bis zur endgültigen Ausführung der eigentlichen Schadsoftware auf einem Endgerät mehrere Phasen.

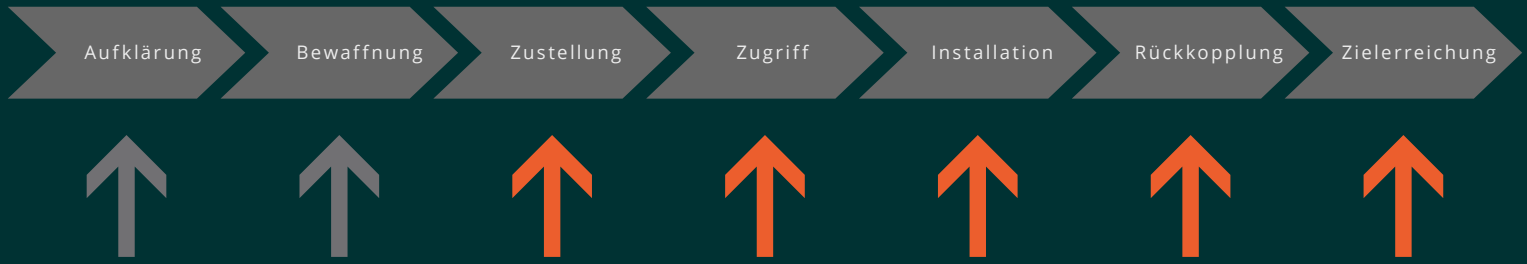
In diesem E-Book erläutern wir all dies näher und erklären, mit welchen Tricks und Techniken das organisierte Cyberverbrechen arbeitet, um Unternehmensnetzwerke unter seine Kontrolle zu bekommen. Wenn Sie wissen möchten, was Sie im Ernstfall tun können, müssen Sie zuverlässig erkennen, wann Gefahr im Verzug ist – je früher, desto besser.



„Auf den Zusammenhang zwischen Exploit, Trojaner und Payload kommt es an.“

„Das Angebot der meisten MSPs und IT-Serviceprovider geht über Gefahrenerkennung und -analyse nicht hinaus.“

CYBER KILL CHAIN VON LOCKHEED MARTIN



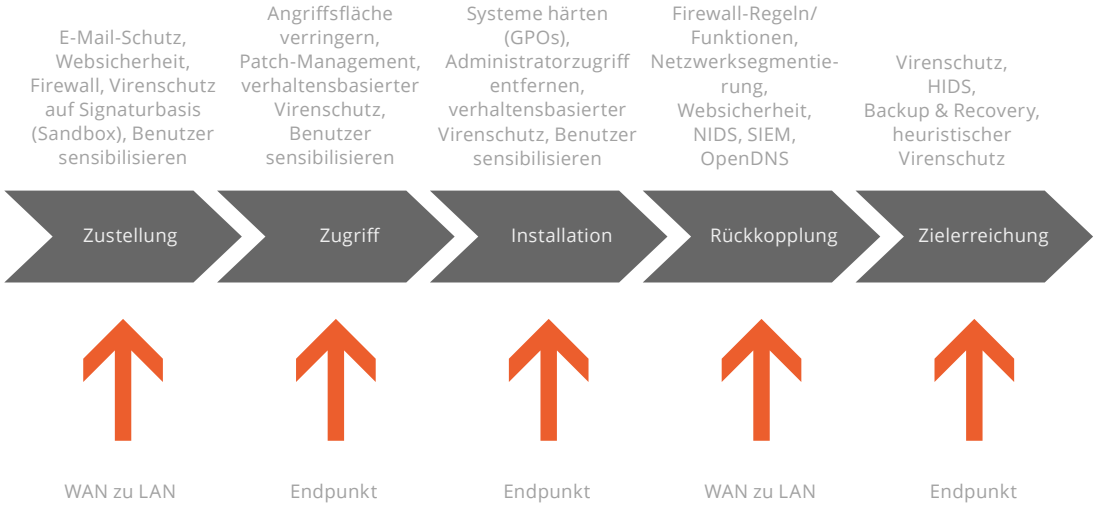
Die ursprüngliche Cyber Kill Chain von Lockheed Martin hat zwei weitere Stufen: „Aufklärung“ und „Bewaffnung“ (hier mit grauen Pfeilen gekennzeichnet). Die Mittel, Angreifern auf diesen beiden Stufen etwas entgegenzusetzen, haben in der Regel nur die ganz großen Anbieter. Das Angebot der meisten MSPs und IT-Spezialisten beschränkt sich wohl eher auf Gefahrenerkennung und -analyse.

Je besser die Branche die Mechanismen hinter verbrecherischen Hacks verstehen lernt, desto eher wird sich mit lernenden Systemen und künstlicher Intelligenz auch in den ersten beiden Phasen der Kill Chain ansetzen lassen. Noch ist das aber Zukunftsmusik; im Moment sind die Möglichkeiten hier sehr eingeschränkt.

Festzustellen bleibt: Die geopolitische und wirtschaftliche Entwicklung der Welt wird die Internetkriminalität weiter verschärfen. Einzeltäter und organisierte Banden werden weiter soziale Netze durchforsten, Schwachstellen ausfindig machen, sich immer neue Malware und Tricks ausdenken, um ihre Opfer zu erpressen oder zu schädigen.

ANGRIFFSMECHANISMEN VERSTEHEN

CYBER KILL CHAIN (NACH LOCKHEED MARTIN)



Oberhalb der Kill-Chain-Kettenglieder sind diverse (längst nicht alle!) Maßnahmen aufgeführt, mit denen in der betreffenden Phase reagiert werden kann. Unter den grauen Feldern, die für die einzelnen Angriffsphasen stehen, sehen Sie, wo genau im Netzwerk angesetzt werden muss, um weitere Entwicklungen zu verhindern oder bereits erfolgte Schäden zu beheben.

„In vielen Ländern erfolgt die Zuweisung von IP-Adressen dynamisch. Dieser Umstand nutzt auch den Kriminellen.“

Gefahrenerkennung und -analyse sind keine triviale Angelegenheit, denn es geht hier um weitaus mehr als das Blacklisting von IP-Adressen und eine stets aktuelle Firewall. In vielen Ländern erfolgt die Zuweisung von IP-Adressen dynamisch. Was heute auf einer Blacklist steht, kann morgen schon wieder harmlos sein; auch wird manche Malware durch Aufräumarbeiten eines Systemadministrator en passant gelöscht. Ohne weiteren Kontext ist nicht zu sagen, welche IP-Adresse zu einem bestimmten Zeitpunkt sinnvollerweise blockiert werden sollte.

Wer auch in den ersten beiden Phasen der Cyber Kill Chain reagieren können möchte, sollte sich eine so genannte Honeypot-Umgebung einrichten, die potenzielle Angreifer anlocken und vom Unternehmensnetzwerk ablenken soll und dabei verdächtige Vorgänge sichtbar machen kann. Die moderne Bedrohungserkennung und -analyse liefert zwar jede Menge Daten, doch vieles davon ist kontextlos. Einem Unternehmen, das weder mit Südkorea noch Russland zu tun hat, nützt die Information, dass eine südkoreanische IP-Adresse gerade ein russisches Netzwerk angreift, gar nichts. In einer Honeypot-Umgebung lassen sich derlei Daten aus aktuellen Angriffen aber sammeln und auswerten, um sich gegen künftige, ähnlich gelagerte Herausforderungen wappnen.

BEDROHUNGEN RICHTIG EINSCHÄTZEN

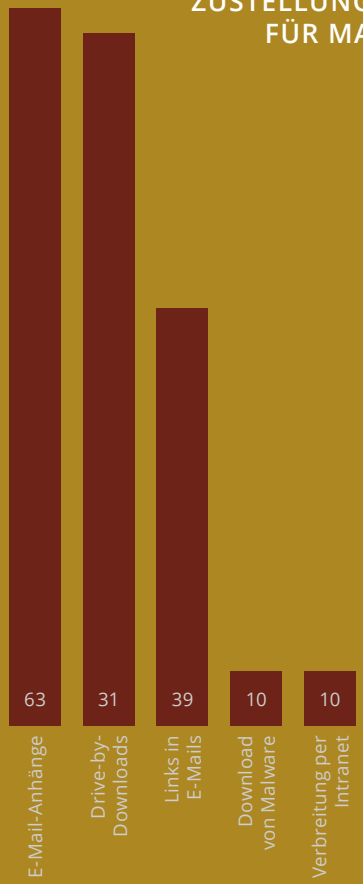
„Einem Unternehmen, das weder mit Südkorea noch Russland zu tun hat, nützt die Information, dass eine südkoreanische IP-Adresse gerade ein russisches Netzwerk angreift, gar nichts.“

Mit den Budgets und Ressourcen, die MSPs, IT-Serviceprovider und Unternehmen üblicherweise bereitstellen können, bleiben machbare Schutzkonzepte auf die letzten fünf Phasen der Cyber Kill Chain beschränkt; für mehr bedürfte es entsprechender Investitionen in Technik und Spezialhardware.

Die erste praktikable Gelegenheit zu einer technisch gestützten Intervention besteht in der Zustellungsphase eines Angriffs. Das Balkendiagramm auf Seite 13 stammt aus dem Verizon Data Breach Investigations Report von 2016 und zeigt die häufigsten Einfallstore für Schädlinge.[2]

Das gute alte Phishing verfängt nach wie vor: Der Anteil geöffneter Phishing-Mails liegt bei erschreckenden 30 %[3]. In der Schlacht gegen kriminelle Hacker bleiben verseuchte Dateianhänge und E-Mail-Links also ein Hauptschauplatz. Gleich auf Platz zwei – noch vor den E-Mail-Links – steht ungeschütztes Surfen im Internet. Weiterhin gilt also: Um bereits in der Zustellungsphase zu intervenieren, bedarf es E-Mail- und Webfiltermechanismen und der Aufklärung und Sensibilisierung der Netzwerkbenutzer.

DIE FÜNF HÄUFIGSTEN ZUSTELLUNGSWEGE FÜR MALWARE



VERTEIDIGUNGSLINIE CLOUD-SERVICE

Gmail, Office 365 und andere Cloud-Angebote gehören inzwischen zum Online-Alltag und sie ermöglichen Unternehmen eine kostengünstige Abwehr von Angreifern in der Zustellungsphase. Die Einrichtung der Verteidigungslinie Cloud-Service ist höchst simpel und berührt den laufenden Geschäftsbetrieb überhaupt nicht. Mögliche Maßnahmen an diesem Punkt sind E-Mail-Scans und die Einrichtung von Proxy-Services für sicheres Surfen – entweder im eigenen Rechenzentrum oder per Cloud.

Der große Vorteil von Cloud-Services: Sie liegen weit außerhalb des Netzwerks und hebeln Angriffsversuche auf Endgeräte frühzeitig aus. Gegen manches sind jedoch auch ihre Viren-Engines und heuristischen Funktionen machtlos: all die Tricks nämlich, mit denen Systembenutzer immer wieder übertölpelt werden und auf einen bestimmten Link klicken oder ein verseuchtes Datenpaket ausführen.

Der spurenlose Einbruch in geschäftliche E-Mail-Systeme über dateilose Malware, auch „Chefbetrug“ genannt, ist ein solcher Trick, den selbst schärfste Filter nicht erkennen. Dieser besonders hinterhältigen Spielart des Social Engineering ist nur durch Sensibilisierung der Systembenutzer beizukommen. Sie müssen angewiesen werden, sich beim angeblichen Urheber eines ihnen verdächtig erscheinenden Anliegens rückzuversichern.

„Mails vom Chef“ haben eine noch bessere Erfolgsquote als Ransomware-Erpressung, schließlich werden Anweisungen des eigenen Vorgesetzten von vielen Mitarbeitern nun mal nicht hinterfragt – auch dann nicht, wenn es um einen Geldtransfer geht.

„Der große Vorteil von Cloud-Services: Sie liegen weit außerhalb des Netzwerks und hebeln Angriffsversuche auf Endgeräte frühzeitig aus.“

Die „Mail vom Chef“ lässt sich auch für andere Zwecke als illegale Geldtransfers nutzen, zum Beispiel zum Diebstahl von Personaldaten. In einer Umfrage eines SIEM-Anbieters gab gut ein Drittel an, ihre Vorgesetzten seien schon auf „Mails vom Chef“ hereingefallen. Und gut 80 % der Befragten befürchteten, ihr Vorgesetzter könnte eines Tages auf so etwas hereinfallen.
Diese Bedenken sind nur zu berechtigt: Alleine im vergangenen Jahr wurden in den USA über Chefbetrug bei über 50 Unternehmen, darunter Snapchat und Care.com, Einkommens- und Steuerdaten von Mitarbeitern erbeutet.[4]

Alle technischen Register zu ziehen, damit es ein Angriff erst gar nicht tief ins Netzwerk hinein schafft, ist wichtig. Bei täuschend echt aussehenden E-Mails von Kriminellen ist und bleibt die Sensibilisierung der eigenen Mitarbeiter für Sicherheitsfragen aber die schlagkräftigste Gegenmaßnahme, die ein Unternehmen ergreifen kann.

TEIL 2—VIRENSCHUTZ UND PATCH-MANAGEMENT

In diesem Abschnitt geht es um die Phase „Zugriff“ der Cyber Kill Chain: das Einschleusen von Malware über Schwachstellen im Netz nach erfolgter „Zustellung“. Die Zugriffsphase zielt nun auf Endpunkte im Netz ab.

Das Exploit-Kit, das wirksam werden soll, findet sein Angriffsziel – den Endpunkt – in einem von vier Zuständen vor, die wir im Folgenden schildern werden.

„Brute-Force-Angreifer beißen sich an der Windows-Authentifizierung die Zähne aus, da sie nach einer bestimmten Anzahl gescheiterter Login-Versuche den Zugriff blockiert.“

ZUSTAND 1: SYSTEM VOLLSTÄNDIG GEPATCHT, VIRENSCHUTZ INSTALLIERT UND AKTUELL

Hier sind die einzigen Schwachstellen menschliches Versagen (Benutzer lässt sich austricksen und installiert Malware) oder ein Angriff per Zero-Day-Exploit, den der Virenscanner nicht erkennt.

Die einzig wirksame Waffe gegen subtiles Social Engineering ist die Aufklärung der Systembenutzer, denn je unwissender oder gutgläubiger sie sind, desto besser lässt sich Schadsoftware einschleusen, etwa ein Visual-Basic-Makro, „zugestellt“ per Phishing-Mail. Mit aktuellen Malware-Signaturen und heuristischer und verhaltensbasierter Analyse von Exploit-Aktivitäten lassen sich Endpunkte im Netzwerk schützen, allerdings nicht immer.

SCHUTZZUSTAND: **GRÜN**

ZUSTAND 2: SYSTEM NICHT GEPATCHT, VIRENSCHUTZ INSTALLIERT UND AKTUELL

Hier bestehen die Schwachstellen in Exploits, die es auf Lücken im Patching abgesehen haben. In diesem Fall nutzt es nichts, wenn die Virensoftware aktuell ist. Sie erkennt den Exploit im Zweifelsfall trotzdem nicht. Schafft er es aber erst einmal am Virenscanner vorbei, so läuft das System Gefahr, infiziert zu werden. Untersuchungen von Recorded Future zufolge sind Adobe Flash, Java und der Internet Explorer die beliebtesten Zielscheiben für Exploit-Kits.[5] Der beste Schutz ist es also, Software, die solche Schwachstellen aufweist, gar nicht erst zu installieren.

SCHUTZZUSTAND: **GELB**

„Schafft ein Exploit es am Virenscanner vorbei, so besteht große Infektionsgefahr für das System."

ZUSTAND 3: SYSTEM NICHT GEPATCHT, VIRENSCHUTZ INSTALLIERT, ABER NICHT AKTUELL

Hier sind die Sicherheitslücken wesentlich größer als bei Zustand 1 und 2, da das System älteren wie jüngeren Exploits Angriffsfläche bietet. Wie in Zustand 2 kann es auch hier leicht zu einer Infektion kommen – und höchstwahrscheinlich zu weiteren Wiederholungen. Vielen IT-Anbietern und MSPs ist dieses Szenario leider allzu vertraut. Wichtig ist hier in erster Linie ein vernünftiges Patching, weil ungepatchte Systeme für das Einbringen von Schadcode per Trojaner besonders anfällig sind. Ein schlagkräftiger Antivirenschutz ist mit aktuellen Malware-Signaturen ausgestattet; verhaltensbasiert und heuristisch agierende Erkennungs-Engines halten nach allem Ausschau, was potenziell verdächtig sein könnte: ein Anschwellen des Datenstroms in Richtung ganz bestimmter IP-Gruppen oder der Aufruf von Javascript aus einem E-Mail-Anhang. Ungewöhnliche Aktionen und Ereignisse können ein Indiz dafür sein, dass sich gerade ein Trojaner auf einem Endpunkt einnistet.

SCHUTZZUSTAND: **ROT**

„Ungewöhnliche Vorgänge im Netzwerk können ein Indiz dafür sein, dass sich gerade ein Trojaner auf einem Endpunkt einnistet.“

ZUSTAND 4: SYSTEM GEPATCHT, VIRENSCHUTZ INSTALLIERT, ABER NICHT AKTUELL

Dieser Zustand ist ähnlich Zustand 1, jedoch gerade deshalb so gefährlich, weil das Patching zwar viele – aber eben nicht alle – Lücken zu schließen vermag. Die Angriffsfläche entspricht der von Zustand 1, aber ein solches System ist für alle möglichen Trojaner anfälliger, kann also durch menschliches Versagen Schaden nehmen. Angriffe haben hier typischerweise direkt nach einem frischen Patching von Endgeräten Erfolg. Das Patching gaukelt bis zu einem gewissen Grad falsche Sicherheit vor, doch die Bedrohung durch Trojanerbefall per E-Mail bleibt. Das Problem: Ist der Virenscanner auf dem Opfersystem nicht aktuell, so stehen hier nicht nur den neuesten, sondern auch noch vielen älteren Trojanern die Türen offen.

SCHUTZZUSTAND: **GELB**

„Das System ist anfälliger für menschliches Versagen.“

Sowohl in Zustand 3 als auch 4 ist der Virenschutz nicht aktuell. Hier wäre es dringend angesagt, die Signaturen zu aktualisieren und alle Endpunkte auf Befall hin zu scannen. Die Wahrscheinlichkeit einer Malware-Infektion bei nicht aktuellem Virenschutz ist sehr hoch. Wer gibt schon gerne zu, dass er etwas angeklickt oder geöffnet und sich darüber einen Trojaner eingefangen hat, der nur deshalb nicht sofort eine Payload herunterlädt, weil er von anderen Verteidigungsmaßnahmen in Schach gehalten wird?

Bei Spezialsoftware für die Gehaltszahlung, Buchhaltung oder Kassensystemen sind folgende Maßnahmen indiziert: Entfernung aller nicht benötigten Exploit-anfälligen Programme, wöchentliches Patching und Aktualisierung benötigter, Exploit-anfälliger Programme (z. B. Adobe Flash). Natürlich kann nicht jede gefährdete Software entfernt werden. Umso mehr braucht es einen zuverlässigen Virenschutz, dessen Signaturen regelmäßig aktualisiert werden, und eine verhaltensbasierte und heuristische Analyse von Daten, um ausreichend geschützt zu sein.

Von der Sensibilisierung der Netzwerkbenutzer abgesehen liegt der Schwerpunkt dessen, was MSPs und IT-Serviceprovider anbieten können, auf den hier beschriebenen Maßnahmen. Entscheidend ist ein zügiges Testen und effizientes Einspielen von Patches ins Netzwerk. Virenschutzsignaturen stets aktuell zu halten, ist sicherlich auch wichtig, hat aber keine erstrangige Priorität.

Oberste Priorität hat ein solides Datensicherungskonzept, gefolgt von Patching. Nur so lassen sich Kriminelle vom eigenen Netzwerk fernhalten.

TEIL 3—ANGRIFFSFLÄCHE VERRINGERN UND NACH MALWARE-INDIZIEN SUCHEN

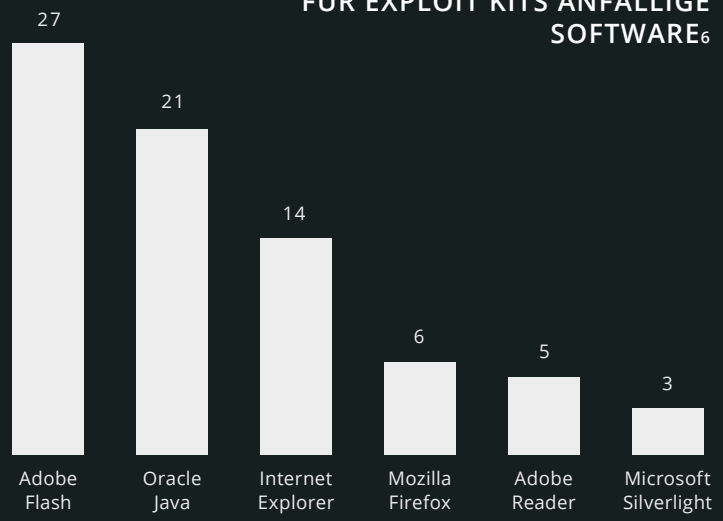
Die Grafik unten rechts zeigt deutlich: Software zu entfernen, die eine ausgesuchte Zielscheibe von Hackern ist, steigert die Sicherheit enorm und ist vor allem dann wichtig, wenn Endgeräte nicht engmaschig gepatcht werden können. Wofür es verschiedene Ursachen geben kann: Vielleicht fehlt es an Automatismen und Tools dafür oder man fürchtet, sein eigenes System durch Fehler beim Patchen versehentlich lahmzulegen. Oft ist der IT das Thema auch schlicht nicht präsent oder es passt nicht in vorhandene Arbeitsroutinen.

Doch lässt sich ohne große technische Investitionen mehr Sicherheit schon alleine dadurch schaffen, dass die Installation und Nutzung der „gefährlichen 5“ (Adobe Flash, Java, Internet Explorer, Firefox und Silverlight) an eine Berechtigung dafür gekoppelt wird. Das Infektionsrisiko für Endpunkte in Unternehmensnetzwerken sinkt beträchtlich, wenn Adobe Flash, Java oder der Internet Explorer generell verboten werden oder deren Benutzer verpflichtet werden, die Programme stets auf aktuellem Stand zu halten.

Befinden sich auf einer Workstation die besagten Anwendungen gar nicht, so kann ein Exploit dort u. U. nichts ausrichten, da er schlicht keine Angriffsfläche findet. Gut zu wissen für regulierte Branchen oder Unternehmen, die hohen Wert auf die Vertraulichkeit und Integrität ihrer Datensysteme legen.

In Teil 1 ging es darum, wie man der Zustellung von Trojanern und Payloads vorbauen kann: durch signaturbasierten Virenschutz auf Endgeräten, Filterfunktionen für Web und E-Mail und eine solide Sicherheitsschulung der Benutzer. Doch Virenschutz auf Endgeräten, Verhaltensanalyse und Benutzerschulungen machen sich auch in der Zugriffsphase der Cyber Kill Chain bezahlt.

FÜR EXPLOIT KITS ANFÄLLIGE SOFTWARE[6]



„Gut zu wissen für regulierte Branchen oder Unternehmen, die hohen Wert auf die Vertraulichkeit und Integrität ihrer Datensysteme legen.“

SIGNATURBASIERTE VIRENERKENNUNG

Bei dieser Methode werden die entdeckten Dateien mit Malware-Signaturen verglichen (Hash-Algorithmen MD5 oder SHA-1), um zu sehen, ob es sich um einen bereits bekannten Schädling handelt. Manche Virenscanner können auch in den Dateien selbst nach Malware-Indizien suchen. Bei Übereinstimmung mit einer Signatur wird die fragliche Datei normalerweise in Quarantäne gestellt.

Entwickler von Exploits und Trojanern wissen, dass ihre Programme irgendwo auf eine Antivirensoftware stoßen werden, und bauen deshalb häufig Code ein, der den Virenschutz ausschaltet und seine Online-Aktualisierung verhindert. In hochspezifischen Angriffen wird installierte Antivirensoftware sogar dazu missbraucht, Schadsoftware zu installieren. Im Mai 2016 ermittelte der Sicherheitsspezialist Tavis Ormandy einen sicherheitstechnisch gefährlichen Pufferüberlauf in „der zentralen Symantec Antivirus Engine, die in den meisten Antivirenprogrammen von Symantec und Norton eingesetzt wird“.[6]

„Bei Übereinstimmung mit einer Signatur wird die fragliche Datei normalerweise in Quarantäne gestellt.“

VIRENSCANNER MIT VERHALTENSANALYSE

Bei dieser Methode hält der Virenscanner nach Indizien für Malware Ausschau und vergleicht diese mit einer Liste von Verhaltensweisen bereits bekannter Schädlinge. Ruft ein als E-Mail-Anhang zugestelltes Dokument bei seiner Öffnung beispielsweise Javascript oder Adobe Flash auf, so kann dies als „äußerst verdächtiges oder Malware-typisches Verhalten“ eingestuft werden.

Die Ermittlung von Verhaltensmustern ist erforderlich, da die Kriminellen ihr Vorhaben verschleiern durch den Einsatz polymorphen oder verschlüsselten Codes – für beides lassen sich Hash-Algorithmen nur sehr schwer erzeugen. Besser entlarven lässt sich Schadsoftware dieser Art, indem nach bestimmten Mustern Ausschau gehalten wird.

Am besten ist es ohne Frage, wenn Exploits, Trojaner und schädliche Payloads das Netzwerk gar nicht erst erreichen.

Doch sollte die äußerste Linie einmal versagen, kann man sich immer noch gegen gezielte Angriffe und versehentlich eingefangene Schädlinge zur Wehr setzen: besonders anfällige Software entfernen, einen Virenscanner mit Verhaltensanalyse betreiben, Systeme regelmäßig patchen und auf ein sicheres Benutzerverhalten achten.

„Sobald sich ein Schädling auf einem Endgerät im Netzwerk eingenistet hat, holt er sich beim Command-and-Control-Server eines Botnetzes weitere Handlungsanweisungen.“

Sobald sich ein Schädling auf einem Endgerät im Netzwerk eingenistet hat, holt er sich beim Command-and-Control-Server (C&C) eines Botnetzes weitere Handlungsanweisungen. Ein zuverlässiges Firewall-Konzept, die Protokollierung von Systemaktivitäten und Netzwerkzugangskontrolle schaffen an diesem Punkt Abhilfe: Sie ermitteln infizierte Endgeräte und können die weitere Ausbreitung der Infektion stoppen.

Seine C&C-Infrastruktur baut ein Botnetz aus zuvor infizierten Servern und Workstations auf. Botnetze lassen sich bei organisierten Kriminellen im so genannten CaaS-Verfahren (Crime as a Service) anmieten; auf Wunsch werden sie auch für die Ausführung ganz gezielter Angriffe maßgeschneidert. Praktisch alle modernen Schädlinge müssen sich mit einer Kommandozentrale verbinden, um die eigentliche Aktion ausführen zu können. Es mag unglaublich klingen, aber so wie normale Unternehmen die Online-Interaktion mit ihren Kunden verfolgen, erheben auch Cyberkriminelle jede Menge Metadaten zu ihren Angriffen: Infektionsrate, geografische Verteilung, Systemdaten. All dies wird zu CaaS-Marketingzwecken erfasst.

Unten sehen Sie ein Beispiel zur Netzwerkkommunikation eines Trojaners. Sein C&C-Server hat die feste Adresse *twinpeakshockey.com*. Der Trojaner verbindet sich mit dieser Domain über eine DNS-Standardabfrage (erste blaue Zeile). Dann versucht er, die Schadsoftware *GORsjo.exe* vom Server zu erhalten (Befehl „GET“, vorletzte Zeile in grün).

Die Kommunikation erfolgt hier ganz offen und unverschlüsselt per HTTP-Protokoll. Die meisten Webfilter würden einen Endgerätezugriff auf die unter der IP-Adresse 69.89.31.222 erreichbare Domain als gefährlich einstufen und davor warnen. Mit DNS-Schutzmechanismen wie OpenDNS und ähnlichen Lösungen ließe sich sogar Malware entlarven, die zur Kommunikation HTTPS nutzt. Und der Download von Schadsoftware in Form von EXE-Dateien auf Endgeräte würde von Firewall oder Webschutz ganz sicher vereitelt.

KOMMUNIKATION ZWISCHEN TROJANER UND C&C-SERVER

11	4.177967	8.8.8.8	172.16.25.137	ICMP	Echo (ping) reply (id=0x0200, seq(be/le)=7168/28, ttl=128)
12	25.196459	172.16.25.137	172.16.25.2	DNS	Standard query A twinpeakshockey.com
13	25.674355	172.16.25.2	172.16.25.137	DNS	Standard query response A 69.89.31.222
14	25.676099	172.16.25.137	69.89.31.222	TCP	iascontrol-oms > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
15	25.676823	69.89.31.222	172.16.25.137	TCP	http > iascontrol-oms [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16	25.676879	172.16.25.137	69.89.31.222	TCP	iascontrol-oms > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
17	25.677229	172.16.25.137	69.89.31.222	HTTP	GET /GORsjo.exe HTTP/1.1
18	25.677524	69.89.31.222	172.16.25.137	TCP	http > iascontrol-oms [ACK] Seq=1 Ack=188 Win=64240 Len=0

WIRKSAME VERTEIDIGUNGSLINIEN

„Firewall-Regeln unterbinden die Rückkopplung von Trojanern mit einem C&C-Server und verhindern das so genannte Lateral Movement, bei dem sich Angreifer quer durchs Netzwerk bewegen und immer neue Endgeräte infizieren.“

An diesem Punkt obligatorisch sind die Netzwerksegmentierung, ein per Firewall geregelter ausgehender Datenverkehr und ein gutes Ereignis- und Protokollmanagement mit Warnfunktion. Das Firewall-Regelwerk muss selbstverständlich auf die Erfordernisse der Geschäftsservices abgestimmt werden (Öffnung von Ports).

Mit dem unten dargestellten Grundgerüst lässt sich zum einen die Kontaktaufnahme von Trojanern mit einem C&C-Server unterbinden und zum anderen verhindern, dass Angreifer sich per Lateral Movement durchs Netzwerk bewegen und immer neue Endgeräte infizieren.

- Ablehnungsregeln für Workstation-Subnetze: keine ausgehender Datenverkehr zu DNS, IRC, NTP, FTP, ICMP, SMTP, SNMP, RDP
- Ablehnungsregeln für Admins (Aufhebung nach Bedarf): keine ausgehender Datenverkehr zu DNS, IRC, NTP, FTP, ICMP, SMTP, SNMP, RDP
- Ablehnungsregeln für Drucker-Subnetze: alle Datenverkehre ablehnen. Kein Internetanschluss für Drucker!
- Ablehnungsregeln für Server: nur DNS, NTP an bestimmte IPs, HTTPS.

Wie Sie sehen, lassen sich durch Einrichtung einer wirksamen Kontrolle von Ports, Protokollen und Datenpaketen – netzwerkintern und ein-/ausgehend – auf Architekturebene verdächtige oder nicht berechtigte Netzwerkaktivitäten zuverlässig erkennen und verhindern.

Der Versuch eines Trojaners beispielsweise, sich per IRC-Protokoll mit seinem C&C-Server rückzukoppeln, würde mit diesen Regeln vereitelt. Wäre ein SIEM-System installiert, so würde dazu noch eine Warnung ausgegeben.

UNTERBINDUNG VON LATERAL MOVEMENT

SERVER
192.168.2 X
SAN/NSA Dateifreigabe, per https, Ereignisproto-kollierung, HIDS/HIPS.

FIREWALL
192.168.1 X
Kommunika-tions-regeln, Auf-spürungs-regeln, WAP in DMZ.

BENUTZER
192.168.4 X
GPO: No Coms. xxx
192.168.4 X
Lokaler Admin für MAX & Mgt.

DRUCKER
192.168.5 X

ADMINS
192.168.3 X
Keine Admin-E-Mail, Ereig-nisprotokollie-rung, HIDS/HIPS.

WIRKSAME VERTEIDIGUNGSLINIEN

Ein weiteres Beispiel ist die reguläre Ablehnung von SMTP-Datenverkehr auf Workstations. Sie verhindert, dass ein befallener Endpunkt in ein Spam-Botnetz eingebunden und für die Aussendung von trojanerbehafteten Phishing-Mails missbraucht wird.

Alle internen und externen Kommunikationsversuche von Trojanern wiederum werden durch die Kombination aus Firewall-Regeln, Netzwerksegmentierung und SIEM-Protokollierung/ Warnmeldungen entweder entdeckt oder verhindert.

Für MSPs und IT-Anbieter lohnt es sich, Kunden ein Sicherheitspaket aus genau diesen Bausteinen anzubieten.

Viele Netzwerke lassen sich auch ohne infrastrukturellen Umbau segmentieren und mit einem tauglichen Firewall-Regelwerk ausstatten. Wird dann noch ein SIEM-Ereignismanagement integriert, das Regelverstöße von Endpunkten unverzüglich meldet, so kann im Bedarfsfall jederzeit zügig reagiert werden. Dieses Konzept dürfte Kunden von MSPs überzeugen.

„Durch Netzwerksegmentierung und Regelung des ausgehenden Datenverkehrs per Firewall sichern MSPs die Netzwerke ihrer Kunden wirksam ab.“

TEIL 5—REAKTION IM ERNSTFALL

Und wenn es nun doch passiert? Ein Exploit dringt ins Netzwerk ein und schleust einen Trojaner auf eine Workstation. Dieser verbindet sich mit einem Botnetz und lädt eine Schadsoftware herunter.

Wie wir gesehen haben, lässt sich im Idealfall auf jeder Stufe in der Cyber Kill Chain der feindlichen Übernahme eines Netzwerks vorbeugen. Doch die Welt ist selten ideal, und viele Unternehmen, die schon Opfer einer Ransomware-Erpressung waren, können davon ein Lied singen.

Malware gibt es in vielen Spielarten und mit unterschiedlicher Funktionsbandbreite. Manche Schädlinge sind echte Grobiane, die Systeme sehr offensichtlich manipulieren, andere hinterlassen bei ihrem heimtückischen Treiben fast keine Spuren. Ransomware gehört in die erste Kategorie: Sie verschlüsselt die Dateien auf dem befallenen System einfach – fertig. Ihre Achillesferse sind heuristische Systeme, die Ransomware sehr schnell aufspüren können.

In einer normalen Geschäftsumgebung mit sich tendenziell vorhersagbar verhaltenden Endgeräten fällt Ransomware mit ihrem untypischen Treiben sofort aus dem Rahmen. Eine sprunghaft ansteigende und danach dauerhaft hohe CPU-Aktivität und massenhafte Schreibzugriffe auf Dateien in Workstation- oder Netzwerklaufwerken werden von einem guten Virenschutz mit Heuristik sofort erkannt. Hält diese Aktivität an, werden die zugehörigen Prozesse schlicht abgebrochen.

Software mit Heuristikfunktion hält genau nach solchen Verhaltensmustern Ausschau. Aus Systemperspektive ist Ransomware eher ein Elefant im Porzellanladen, der sogar auf der Netzwerkschicht den Datenverkehr anschwellen lässt und massenhaft Lese-/Schreibanfragen vom infizierten Endpunkt an den Server generiert.

„Im Idealfall wird auf jeder Stufe der Cyber Kill Chain der feindlichen Übernahme eines Netzwerks vorgebeugt. Doch die Welt ist selten ideal.“

DIE LETZTE VERTEIDIGUNGSLINIE

Sogar im Ernstfall ist noch nicht alles verloren; die Auswirkungen eines Angriffs lassen sich durchaus mindern, zum Beispiel über Gruppenrichtlinienobjekte (GPOs) oder externe Anwendungen zum Sperren bestimmter Verzeichnisse wie „%App/Data“ und „%App/User“, damit darin befindliche Dateien nicht ausgeführt werden können. Sehr hilfreich ist hier das Ransomware Prevention Kit von Third Tier.[8]

In modernen Windows-Active-Directory-Umgebungen kann über Whitelisting mit dem AppLocker oder einem vergleichbaren externen Tool die Ausführung von Erpressersoftware wirksam verhindert werden. Weitere Informationen zum Einsatz des AppLockers gegen Ransomware finden Sie im Technet Blog (Quelle 9, siehe Seite 45). Das Ganze funktioniert, indem die Benutzer keine Rechte für die Domain- oder lokale Administration erhalten.

Vermutet ein Netzwerkbenutzer nach dem Öffnen eines Mailanhangs oder Besuchen einer Website, dass ein Ransomware-Angriff im Gang ist, so sollte er seinen Computer unverzüglich vom Stromnetz trennen oder den Einschaltknopf so lange drücken, bis der Computer sich ausschaltet. Wenn die Ransomware vom betreffenden Gerät aus ausgeführt werden soll, den Server aber noch nicht erreicht hat, können durch diese Aktion viele Dateien vor bösartiger Verschlüsselung bewahrt werden. Das Gerät sollte so lange aus dem Netzwerk entfernt werden (Wireless-Zugang deaktivieren nicht vergessen!), bis sein Einschalten gefahrlos wieder möglich ist.

Bei Ransomware-Angriffen muss auf zwei Dinge geachtet werden: erstens das infizierte Gerät – es wird sofort nach dem Wiedereinschalten damit beginnen, Dateien zu verschlüsseln, sofern es noch mit dem Netzwerk verbunden ist. Zweitens die verschlüsselten Dateien selbst.

„Sogar im Ernstfall ist noch nicht alles verloren.“

„Zu Aufklärungszwecken sollte das befallene Gerät einer forensischen Spezialuntersuchung unterzogen oder einer Strafverfolgungsbehörde übergeben werden.“

Auf dem infizierten Endpunkt müssen nun Sicherheitslücken geschlossen (Patching, Entfernen der gehackten Software) und der Trojaner sowie die Ransomware gelöscht werden. Verbleibt eines von beiden im System, so kann sich dieses nach Verbindung mit dem Internet wieder neu infizieren und Schadcode herunterladen. Dann geht das ganze Spiel von vorne los. Einer fortgeschrittenen Infektion wird man nur Herr durch Einspielen eines so genannten Golden Image (ISO-Datei) oder eines garantiert einwandfreien Systemabbilds von einem sauberen, separaten Speichermedium aus.

Infizierte Endgeräte enthalten wertvolle forensische Daten. Sie liefern Informationen zu den Angreifern und geben Aufschluss darüber, wie genau das Sicherheitskonzept ausgehebelt wurde. Bei Großangriffen mit erheblicher Auswirkung auf den Geschäftsbetrieb sollten die Betroffenen das befallene Gerät einer forensischen Spezialuntersuchung unterziehen oder einer Strafverfolgungsbehörde übergeben.

Wenn Sie sich dafür entscheiden, das vom Netzwerk getrennte Gerät offline zu säubern, sollten Sie es mit Wireshark auf verdächtige Netzwerkverbindungen (besonders http oder https) hin absuchen, bevor sie es wieder aktivieren und ins Netzwerk einbinden. Leider sind moderne Ransomware-Varianten in der Lage, Anmeldedaten zu stehlen, sodass sämtliche Kennwörter einschließlich der in Browser-Cookies abgelegten vermutlich unbrauchbar geworden sind und deshalb geändert werden sollten.

„Vorsicht beim Upload verschlüsselter Daten, die Vertrauliches enthalten.“

Ransomware-Angriffe machen häufig auch lokal abgelegte Backups unbrauchbar. Klug ist es deshalb, Systembackups in der Cloud zu speichern, denn dann lässt sich im Fall eines Angriffs alles schnell wiederherstellen.

Leider trifft viele Unternehmen (beziehungsweise ihren MSP oder IT-Servicepartner) bei einem Ransomware-Angriff die bittere Erkenntnis, dass ihre Backup-Strategie Lücken hat – für so manches Unternehmen durchaus katastrophal.

Allen Opfern eines Ransomware-Angriffs sei die Website von Heimdal Security ans Herz gelegt, die etwa 100 verschiedene Entschlüsselungsprogramme bietet.[10] Lassen Sie aber auch bei bösartig verschlüsselten Dateien höchste Vorsicht walten: Laden Sie nur solche Dateien zur Entschlüsselung hoch, die keine vertraulichen Daten enthalten.

ZAHLEN? ODER LIEBER NICHT?

„Lösegelder nutzen niemandem. Außer denen, die sie fordern."

2015 löste das FBI Irritationen aus, als einer seiner Ermittlungsleiter dazu riet, bei Cybererpressung klein beizugeben und zu zahlen. Dennoch: Außer denen, die sie fordern, nutzen Lösegelder niemandem. In Einzelfällen mögen die verschlüsselten Daten von solch unfassbarem Wert sein, dass ein Unternehmen oder langjähriges Forschungsprojekt ohne sie ruiniert wäre. Dann ließe sich mit einer Zahlung vielleicht das Allerschlimmste verhindern. Opfer von Ransomware-Angriffen müssen auf jeden Fall die bittere Pille schlucken, mit schonungsloser Härte aufzuklären, warum ihre Datensysteme so schlecht geschützt waren.

Wer einen Ransomware-Trojaner in Ihr Netzwerk einschleust, ist ein Verbrecher – Punkt. Kriminelle Hacker dieses Zuschnitts werden jede Chance nutzen, aus Ihrer Misere noch mehr Kapital zu schlagen. Argumentieren Sie also niemals mit dem Wert der Daten. Sonst steigt am Ende der Preis dafür und Sie tragen mit Ihrem Geld zur Entwicklung von noch besserer Ransomware bei. Das kann nicht in Ihrem Sinne sein.

Ransomware-Erpressung ist organisierte Cyberkriminalität und sollte immer gemeldet werden. In den USA melden Sie Vorfälle einer FBI-Dienststelle[11]. Auch online ist eine Meldung über das Internet Crime Complaint Center möglich[12]. In Großbritannien ist Action Fraud die Anlaufstelle[13], in der EU Europol[14] und in Australien Acorn[15]. All diese Institutionen unterstützen Sie beim Kampf gegen Internetverbrechen.

FAZIT

„System in Gefahr“ von SolarWinds® MSP erläutert die Mechanismen moderner Malware und nennt wirkungsvolle Maßnahmen, zu denen Unternehmen, MSPs oder IT-Serviceprovider zur Verhinderung oder Gegenwehr im Ernstfall greifen können.

Ein Angriff ist blitzschnell geschehen. Ob er Erfolg hat und welche Durchschlagskraft er entwickelt, hängt von vielen Faktoren ab. Ein durchdachtes mehrstufiges Konzept aus Maßnahmen zur Prävention, Erkennung und Bekämpfung kann Ransomware-Angriffe vereiteln und das Netzwerk zuverlässig frei von Schädlingen halten.

REFERENZEN

1 **Lockheed Martin Cyber Kill Chain®**
http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

2 **Verizon Data Breach Investigation Report 2016**
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

3 https://blog.barkly.com/phishing-statistics-2016

4 https://www.alienvault.com/blogs/security-essentials/clicking-with-the-enemy

5 **Recorded Future**
https://www.recordedfuture.com/

6 **Digital Shadows**
https://www.digitalshadows.com

7 **Tavis Ormandy report**
https://bugs.chromium.org/p/project-zero/issues/detail?id=820

8 **Third Tier Ransomware Kit**
http://www.thirdtier.net/ransomware-prevention-kit/

9 **Technet Blog**
https://blogs.technet.microsoft.com/askpfeplat/2016/06/27/applocker-another-layer-in-the-defense-in-depth-against-malware/

10 **Heimdal Security**
https://heimdalsecurity.com/blog/ransomware-decryption-tools/

11 **FBI**
https://www.fbi.gov/contact-us/field-offices

12 **IC3**
https://www.IC3.gov

13 **Action Fraud**
http://www.actionfraud.police.uk/report_fraud

14 **Europol**
https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

15 **Acorn**
https://report.acorn.gov.au/

SolarWinds MSP unterstützt weltweit MSPs jeder Größe dabei, hocheffiziente und profitable Geschäftsfelder aufzubauen, die einen maßgeblichen Wettbewerbsvorteil sichern. Mit integrierten Lösungen, u. a. für Automatisierung, Sicherheit, Netzwerk- und Service-Management vor Ort und in der Cloud, können MSPs ihre Arbeit dank datenbasierter Einblicke schneller und einfacher erledigen. SolarWinds MSP hilft MSPs, sich auf das Wesentliche zu konzentrieren: die Erfüllung ihrer SLAs und den Aufbau eines gewinnbringenden Geschäfts.

RMEB00067DE0417

recycle

Weitere Informationen finden Sie auf **www.solarwindsmsp.com**

solarwinds msp

www.solarwindsmsp.com