Vorbereitung auf totale Zerstörungsangriffe

Die Bedrohungslandschaft hat sich dramatisch verändert. Sind Sie auf die neuen zerstörerischen Angriffe vorbereitet?

Geschrieben von Brin Hymer, Strategic Systems Architect bei Quest® Software, in Zusammenarbeit mit Randy Franklin Smith, Windows- und Active Directory-Sicherheitsexperte

EINFÜHRUNG

IT- und Sicherheitsexperten kämpfen schon lange gegen schwere Bedrohungen. Auf der einen Seite stehen Risiken wie Stromausfälle, Hardwaredefekte und Naturkatastrophen. Auf der anderen Seite sind böswillige Insider und listige Hacker, bewaffnet bis an die Zähne mit Tools und Techniken zum Ausnutzen von Schwachstellen und immer komplexeren Viren sowie Malware und Ransomware.

Die Verteidigung gegen diese Bedrohungen war noch nie einfach, aber die Risiken waren durch verschiedene Faktoren begrenzt. Natürliche Bedrohungen sind geografisch beschränkt, und ein zusätzliches Datacenter an einem weiteren Standort ist eine gute Verteidigung. Menschliche Angreifer haben normalerweise ein bestimmtes Ziel: Zugriff auf Ihre Daten, um sie entweder zu stehlen und weiterzuverkaufen, oder um sie zu verschlüsseln, um Lösegeld zu verlangen. Daher konnten IT-Experten Prioritäten für ihre Datenschutzstrategien aufstellen.

Aber in letzter Zeit haben die Probleme zugenommen - Immer mehr Angriffe zielen auf die totale Vernichtung Ihrer Infrastruktur ab. Leider sind viele Unternehmen völlig unvorbereitet. Dieses Whitepaper behandelt einige der gefährlichsten aktuellen Angriffe und analysiert deren Geschwindigkeit, Umfang und Methoden sowie die besten Strategien, um Ihr Unternehmen vor diesen Angriffen zu schützen.

GESCHWINDIGKEIT UND LEISTUNG ZERSTÖRERISCHER ANGRIFFE

Sie haben bestimmt schon einige der Namen gehört, die nach Science Fiction klingen: NotPetya. Shamoon. Stuxnet. Olympic Destroyer. BlackEnergy. Destover. Wiper. Triton. Aber was geschieht bei diesen zerstörerischen Angriffen wirklich? Lassen Sie uns einige aktuelle Vorfälle genauer betrachten, um ein Gefühl für die Geschwindigkeit und den Umfang zu bekommen, und um zu verstehen, wie wichtig eine gute Verteidigungsstrategie ist.

Stuxnet

Ende der 2000er-Jahre waren Israel und die USA besorgt über das iranische Nuklearprogramm. 2009 produzierte das Land genügend angereichertes Uran, um vermutlich innerhalb eines Jahres zwei Atomwaffen herstellen zu können. Daher begannen Israel und die USA, so die landläufige Ansicht, mit der Entwicklung des ausgeklügelten Computerwurms Stuxnet. Dieser Wurm sollte keine Computer übernehmen oder Daten stehlen, sondern physische Geräte zerstören. Wenn Stuxnet einen Computer infiziert, der mit bestimmten PLC-Steuerungen verbunden ist, die zur Steuerung

Immer mehr Angriffe zielen auf die totale Vernichtung Ihrer Infrastruktur ab. Zu viele Unternehmen sind völlig unvorbereitet.

von Maschinen wie Uranzentrifugen eingesetzt werden, ändert Stuxnet die PLC-Programmierung so, dass die Zentrifugen zu schnell und zu lange laufen. Die PLCs melden weiterhin völlig normale Betriebsparameter, um das abweichende Verhalten vor den Personen zu verbergen, die die Geräte überwachen. Mit der Zeit hat diese Belastung dazu geführt, dass die infizierten Maschinen sich selbst zerstört haben. 2010 wurden mehr als 15 iranische Einrichtungen mit Stuxnet infiziert, und fast ein Fünftel der Uranzentrifugen des Landes wurde zerstört.

Stuxnet war nie darauf ausgelegt, sich außerhalb der iranischen Atomeinrichtungen zu verbreiten, die isoliert und nicht mit dem Internet verbunden waren. Irgendwie gelangte die Malware jedoch ins Internet und begann, sich zu verbreiten. Im Lauf der Zeit änderten andere Gruppen das Virus ab, um andere Organisationen wie Kläranlagen, Kraftwerke, Regierungsbehörden und Unternehmen in den Luftfahrt-, Verteidigungs- und pharmazeutischen Branchen ins Visier zu nehmen. Diese abgeänderten Viren werden manchmal auch die „Söhne von Stuxnet“ genannt. Zu ihnen gehören Duqu, Flame, Havex, Industroyer und Triton.

Shamoon

2012 war ein Ölunternehmen an der Reihe, von einem zerstörerischen Cyberangriff getroffen zu werden. Am 15. August infizierte ein Virus, das später den Namen Shamoon erhalten sollte, drei Viertel der 40.000 Workstations von Saudi Aramco, löschte die Festplatten und zeigte ein Bild einer brennenden US-Flagge an. Obwohl das Unternehmen beteuerte, dass die Ölproduktion und der Förderbetrieb von diesem Angriff nicht betroffen waren und dass das zentrale Netzwerk nur zehn Tage lang offline war, berichtete ein für die Wiederherstellung hinzugezogener Berater, dass Saudi Aramco sein Sicherheitscenter komplett neu aufbauen musste, und dass die Systeme erst nach fünf Monaten wieder vollständig online waren. Er schrieb außerdem, dass dieser Angriff ein kleineres Unternehmen mühelos zum Konkurs gezwungen hätte.

Shamoon verschwand vier Jahre lang aus den Schlagzeilen, aber 2016 wurde eine leicht abgeänderte Version der Malware gegen verschiedene Regierungsbehörden und zivile Einrichtungen in Saudi-Arabien und anderen Golfstaaten eingesetzt. Die zerstörerische Malware zeigte ihre hässliche Fratze erneut Ende 2018, als ihr mehrere Ziele im mittleren Osten zum Opfer fielen.

Diese neue Variante von Shamoon ist noch zerstörerischer als die vorherigen Versionen, da sie alle Dateien von den infizierten Computern löscht und anschließend den Master Boot Record vernichtet, um die Wiederherstellung der Dateien nicht nur schwierig, sondern unmöglich zu machen.

BlackEnergy

2015 fand der erste erfolgreiche Cyberangriff auf ein Stromnetz statt. Im Dezember haben Hacker die BlackEnergy-Malware eingesetzt, um in verschiedene Stromverteilungszentralen in der Ukraine einzudringen und elektrische Systeme vom Netz zu nehmen. Obwohl dieser Angriff nur einige Stunden dauerte und nur etwa 225.000 Kunden betroffen waren, war er ein Beweis dafür, dass kritische Infrastruktur anfällig für Malware ist. Zukünftige Angriffe auf Energieversorger könnten noch viel gravierendere Auswirkungen haben.

NotPetya

Der bisher wohl weitreichendste und teuerste Angriff erfolgte im Jahr 2017. Ein leitender Finanzmitarbeiter in der ukrainischen Niederlassung des internationalen Schifffahrtsgiganten Maersk hatte zuvor eine Routineanfrage gestellt: Er hatte die IT-Abteilung gebeten, die Buchhaltungssoftware M.E.Doc auf einem einzelnen Computer zu installieren. M.E.Doc ist nicht irgendeine beliebige Anwendung, sondern die meistverwendete Steuer- und Buchhaltungslösung für alle Geschäftstreibenden in der Ukraine, daher folgte die IT-Abteilung seiner Bitte. Am 27. Juni begannen die Computer in der Maersk-Zentrale, auszufallen. Laut der Untersuchung hatten staatlich geförderte Hacker die Updateserver für M.E.Doc übernommen und eine Backdoor verwendet, um alle Unternehmen, die die Software einsetzen, mit Malware zu infizieren.

Innerhalb von Stunden war Maersk praktisch lahmgelegt. Alle 150 weltweit verteilten Domänencontroller, mit Ausnahme des Domänencontrollers in Ghana, der glücklicherweise während des Updates offline war, waren ausgefallen. Die Schiffsterminals des Unternehmens in aller Welt waren tagelang gelähmt, zehntausende LKWs wurden zurückgeschickt, und Container voller verderblicher Waren konnten nicht gekühlt werden. Bei der Säuberung mussten 4.000 Server und 45.000 Workstations neu aufgesetzt werden. Ein leitender Maersk-Mitarbeiter berichtete, dass NotPetya das Unternehmen zwischen 250 und

300 Millionen US-Dollar gekostet hat, während andere Insider den Schaden eher höher einschätzen.

Der Schaden war jedoch nicht auf Maersk begrenzt - NotPetya infizierte rasend schnell Unternehmen in aller Welt, von Deutschland über die USA bis nach Tasmanien. Es dauerte lediglich 45 Sekunden, bis NotPetya das Netzwerk einer großen ukrainischen Bank lahmgelegt hatte. Ein Teil einer wichtigen ukrainischen Transportzentrale wurde innerhalb von 16 Sekunden komplett infiziert. Praktisch sämtliche Bundesbehörden der Ukraine kamen zum völligen Stillstand. Der Gesamtschaden wurde auf mehr als 10 Milliarden US-Dollar geschätzt.

Angriffe in der Cloud

Zerstörerische Angriffe sind keineswegs auf lokale IT-Umgebungen begrenzt, obwohl nicht alle bisherigen Vorfälle in der Cloud von Malware mit einem kreativen Spitznamen verursacht wurden. 2014 musste beispielsweise der IaaS-Anbieter Code Spaces nach einem mehrstufigen Angriff auf seine Server Konkurs anmelden. Ein Großteil der Daten, Sicherungen, Computerkonfigurationen und Offsite-Sicherungen des Unternehmens waren teilweise oder vollständig gelöscht worden.

Im Februar 2019 brachen Hacker beim E-Mail-Anbieter VFEmail ein und formatierten sämtliche Laufwerke auf allen Datei- und Sicherungsservern in der US-Infrastruktur des Unternehmens und vernichteten somit sämtliche E-Mail-Daten der US-Kunden. Die Angreifer nahmen auch die IT-Ressourcen des Unternehmens in den Niederlanden ins Visier, wurden jedoch rechtzeitig ertappt, und das Unternehmen konnte einen Teil der Sicherungsdaten retten. Trotzdem wurde bei diesem Angriff praktisch die komplette Infrastruktur des Unternehmens innerhalb weniger Stunden gelöscht. Das Unternehmen hält sich entgegen aller Erwartungen weiterhin durch.

MOTIVE FÜR ZERSTÖRERISCHE ANGRIFFE

Herkömmliche Angriffe erfolgen meistens aus finanziellen Gründen, zum Beispiel um bei einem Ransomware-Angriff Lösegeld für den Verschlüsselungsschlüssel zu fordern, um personenbezogene oder Gesundheitsdaten für Identitätsdiebstahl oder zum Verkauf auf dem Schwarzmarkt abzugreifen, oder um Benutzeranmeldeinformationen für zukünftige Angriffe mit finanziellen Motiven zu stehlen. Hinter zerstörerischen Angriffen stecken oft völlig andere Motive, wie etwa:

- **Politische Motive -** Staatlich geförderte Hacks sind auf dem Vormarsch. Experten gehen beispielsweise davon aus, dass Stuxnet gemeinsam von Israel und den USA entwickelt wurde, um das iranische Atomprogramm zu sabotieren, und dass NotPetya ein politisch motivierter Angriff gegen die Ukraine war. Der Shamoon-Angriff im Jahr 2012 war angeblich ein Teil der iranischen Vergeltungsmaßnahmen für die Beteiligung der USA an Stuxnet. Staatlich geförderte Hacker sind normalerweise extrem gut ausgebildet und finanziert, daher sind ihre Angriffe oft besonders vernichtend.
- **Gesellschaftliche Motive -** Manche Angriffe entstehen aus einem Wunsch nach gesellschaftlichen Veränderungen. Diese Gruppen werden oft als „Hacktivisten“ bezeichnet und führen Denial-of-Service-Angriffe (DoS) gegen Organisationen durch, die nicht mit ihrer Ideologie vereinbar sind. Die Hacktivisten-Gruppe Anonymous ist beispielsweise bekannt für die DoS-Kampagne aus dem Jahr 2010, die PayPal.com in die Knie zwang und die Websites von Visa und MasterCard als Vergeltung dafür störten, dass diese Unternehmen Zahlungen an Wikileaks nach Aufforderung der US-Regierung eingestellt hatten.
- **Rache -** Am anderen Ende des Spektrums steht der vergrätzte Insider. Anfang 2002 entwickelte Roger Duronio, ein IT-Admin bei UBS Paine Webber, beispielsweise eine Logikbombe, die er anschließend mit herkömmlichen Unix-Administratortools auf Tausenden von Systemen verteilte. Anschließend kündigte er und ging direkt zu seinem Börsenmakler, um Leerverkäufe für UBS/PW-Aktien im Wert von 21.000 US-Dollar zu tätigen. Als die Logikbombe wenige Wochen später detonierte, fielen ihr etwa 2.000 Server sowie sämtliche Dateien auf den Servern zum Opfer. Der Schaden war so gravierend, dass die Mitarbeiter Transaktionen und andere Geschäftsvorgänge mit Stift und Papier erledigen mussten. Das Unternehmen gab 3 Millionen US-Dollar allein für Beratungsgebühren aus, um die Systeme wiederherstellen zu können. Duronios Motiv? Angeblich war er enttäuscht von seinem Bonus, der 18.000 US-Dollar unter den 50.000 US-Dollar lag, die er erwartet hatte.

  In Windows-Umgebungen ist es vermutlich noch einfacher für einen vergrätzten privilegierten Mitarbeiter, Schäden anzurichten. Dazu genügt es, Active Directory vom Netz zu nehmen. Ohne AD ist Ihr gesamtes Netzwerk offline, auch ohne jegliche Probleme mit Ihren Servern oder Anwendungen.
- **Ablenkung -** Hacker kombinieren ihren Informationsdiebstahl immer häufiger mit einem zerstörerischen Angriff, um ihre Spuren zu verwischen. Der zerstörerische Angriff kann die forensische Analyse beeinträchtigen und

Es dauerte lediglich 45 Sekunden, bis NotPetya das Netzwerk einer großen ukrainischen Bank lahmgelegt hatte. Der Gesamtschaden des Angriffs aus dem Jahr 2017 wurde auf mehr als 10 Milliarden US-Dollar geschätzt.

die Suche nach den Angreifern erschweren, wodurch ihre Verfolgung verhindert und ihre Vorgangsweise geschützt wird, sodass sie dieselben Techniken auch in Zukunft einsetzen können. Die Olympic Destroyer-Malware lähmte beispielsweise die IT-Systeme vor den offiziellen Eröffnungszeremonien der olympischen Winterspiele 2018 in Südkorea. Olympic Destroyer hat seine Spuren jedoch so effektiv verwischt, dass sich die Forscher nicht sicher sein konnten, ob dieselbe Gruppe oder Gruppen mit anderen Interessen verantwortlich waren, als später im gleichen Jahr sowohl Finanzinstitute als auch Labore zur Abwehr biologischer und chemischer Waffen betroffen waren.

- **Kollateralschaden -** Von zerstörerischen Angriffen ist oft nicht nur das unmittelbare Ziel betroffen, sondern es entstehen auch Kollateralschäden. Obwohl es die Urheber des NotPetya-Angriffs beispielsweise eindeutig auf die Ukraine abgesehen hatten - laut Schätzungen erfolgten 80 % aller Infektionen in der Ukraine - erlitten Unternehmen in aller Welt, inklusive Maersk, gravierende Schäden.

Jedes Unternehmen kann zum Ziel eines zerstörerischen Angriffs oder auch zum Kollateralschaden eines Angriffs auf andere Ziele werden.

METHODIK

Wie Sie gesehen haben, treten zerstörerische Angriffe in verschiedensten Formen auf. Manchmal ist Malware oder ein Virus beteiligt, manchmal auch nur rohe Kraft. Manche Angriffe löschen Daten, andere Angriffe verursachen physische Schäden. Lassen Sie uns die Ausbreitung der Angriffe etwas genauer betrachten.

Erstzugriff

Der erste Schritt bei einem Angriff besteht normalerweise darin, sich Zugang zu Ihrem Netzwerk zu verschaffen. Sie sind vermutlich mit den meisten der unten aufgelisteten Techniken vertraut. Es ist wichtig zu betonen, dass zerstörerische Angriffe nicht nur Computer ins Ziel nehmen, wie etwa Workstations und Server. Zu Ihrer Angriffsoberfläche zählen auch Ihre IoT-Geräte, Router und sonstige Hardware.

- **Phishing -** Shamoon ist in das Netzwerk von Saudi Aramco eingedrungen, als ein Mitarbeiter der IT-Abteilung eine bösartige Phishing-E-Mail geöffnet hat.
- **Backdoor -** Eine Backdoor in der Updatesoftware für eine externe Unternehmenssoftware hat es den Angreifern ermöglicht, Maersk und andere Unternehmen weltweit mit NotPetya zu infizieren.
- **Infiziertes USB-Gerät -** Da die iranischen Atomeinrichtungen nicht mit dem Internet verbunden sind, musste Stuxnet über ein physisches USB-Gerät eingeschmuggelt werden, entweder absichtlich oder versehentlich.
- **Sicherheitslücken in Software -** Eine der beim NotPetya-Angriff sowie beim WannaCry-Ransomwareangriff 2017 eingesetzten Techniken war ein Einbruchstool mit dem Namen EternalBlue, das von der US-Behörde NSA entwickelt und bei einem verheerenden Leak veröffentlicht wurde. EternalBlue nutzt eine Sicherheitslücke in einem bestimmten Windows-Protokoll aus, und Hacker können auf allen ungepatchten Computern nach Belieben ihren eigenen Code ausführen.
- **WLAN- oder Sendestationen-Hijacking -** 2015 musst der Hersteller des Jeep Cherokee 1,4 Millionen Fahrzeuge zurückrufen, nachdem Forscher demonstriert hatten, dass sie die Fahrzeugsysteme über das Internet übernehmen können. Ein Angreifer könnte beispielsweise die Türschlösser und Bremsen, den Motor und den Autopilot unter seine Kontrolle bringen. Die Behörde FDA hat außerdem bestätigt, dass bestimmte Herzschrittmacher-Implantate Sicherheitslücken aufweisen, mit denen ein Hacker den Akku erschöpfen, einen falschen Herzrhythmus vorgeben oder Elektroschocks auslösen könnte.
- **Sicherheitslücken in IoT-Geräten -** Im Oktober 2016 zwang der bisher umfangreichste DDoS-Angriff aller Zeiten große Teile des Internets in die Knie, darunter Twitter, Netflix, Reddit und CNN, indem der Dienstanbieter Dyn angegriffen wurde. Das bei diesem Angriff verwendete Botnet bestand aus einer großen Anzahl von mit dem Internet verbundenen Geräten wie etwa Druckern, Digitalkameras, Babymonitoren und Privatroutern, die mit einer Malware namens Mirai infiziert waren.
- **Sicherheitslücken in anderen Geräten -** Was geschieht, wenn jemand Ihre Router, Firewalls und drahtlosen Zugriffspunkte auf die Werkseinstellungen oder auf andere, speziell gewählte Einstellungen zurücksetzt? Oder siefür eigene Zwecke übernimmt? 2018 forderte das FBI die Verbraucher dazu auf, ihre Router neu zu starten, um die Ausbreitung der Malware VPNFilter einzudämmen, die laut Forschern von einer mit dem russischen Militärgeheimdienst in Verbindung gebrachten Gruppe für koordinierte Cyberangriffe gegen die Ukraine eingesetzt wird. Diese Malware wurde inzwischen verbessert und übersteht einen Neustart. Alle Besitzer der mehr als 70 anfälligen Geräte sind angehalten, die Firmware schnellstmöglich zu aktualisieren.[1]

Ausbreitung im Netzwerk und Schadenswirkung

Sobald die Malware Fuß gefasst hat, verbreitet sie sich vom infizierten Computer auf andere Computer im Netzwerk. Eine Technik verwendet einen Exploit namens Mimikatz, mit

1 Weitere Informationen finden Sie im Fundbericht von Cisco Talus zu VPNFilter sowie in einem Blogeintrag mit einer aktualisierten Liste der betroffenen Geräte. Verwenden Sie Ihre bevorzugte Suchmaschine und andere Nachforschungsoptionen, um sicherzugehen, dass Sie die aktuellsten Informationen erhalten.

dem Hacker die Anmeldeinformationen im Arbeitsspeicher eines Computers auslesen und für den Zugriff auf andere Computer verwenden. Manchmal landet ein Hacker den sprichwörtlichen Jackpot und findet privilegierte Administratoranmeldeinformationen zusätzlich zu den normalen Benutzeranmeldeinformationen. In Unternehmen ohne angemessene Netzwerksegmentierung und andere Grenzen kann sich Malware schnell ausbreiten, und findige Hacker können sich viel einfacher horizontal bewegen. Die Hacker tarnen sich und bleiben dank eines Mangels an fortlaufenden Überwachungs- und Warnmaßnahmen oft unentdeckt.

Anschließend erfolgt der wichtigste Teil des Angriffs. Oft besteht das Ziel darin, entweder bestimmte Daten oder das gesamte Dateisystem zu löschen. Um die Daten zu löschen, überschreiben manche Angriffe gesamte Dateien. Dieser Vorgang ist jedoch zeitaufwändig, und andere Angriffe verwenden schnellere und ebenso effektive Methoden. Ein Angriff kann beispielsweise alle paar Megabyte einen Block von 500 Byte überschreiben, oder einfach die ersten N Byte in einer Datei überschreiben, um die Headerinformationen zu löschen. In beiden Fällen werden die Dateien unbrauchbar gemacht, ohne sie komplett zu löschen. Andere Arten von zerstörerischer Malware greifen das Boot-Subsystem (BIOS) an oder sind darauf ausgelegt, Geräte zu deaktivieren.

Der Angriff wird oft erst ausgelöst, wenn die Malware einen Sättigungszustand erreicht, um zu verhindern, dass das Opfer den Angriff rechtzeitig erkennen und abwehren kann. Um auffällige und leicht erkennbare E/A-Signaturen zu vermeiden, überlässt die Malware die Hauptarbeit oft dem Bootloader. Außerdem werden Angriffe zeitgesteuert ausgeführt, um den Schaden zu maximieren; NotPetya und Shamoon wurden ausgelöst, als viele Mitarbeiter nicht im Büro waren, um sich auf nationale oder religiöse Feiertage vorzubereiten. Auf diese Weise sinkt die Chance, dass der Angriff schnell erkannt wird, und die Opfer haben weniger Chancen, sich zu verteidigen.

VERMEIDUNGS- UND ERKENNUNGSSTRATEGIEN

Da jedes Unternehmen Ziel eines zerstörerischen Angriffs oder auch zum Kollateralschaden eines Angriffs auf andere Ziele werden kann, müssen alle Unternehmen Maßnahmen ergreifen, um ihre Risiken zu senken. Der erste Schritt ist die Implementierung standardisierter Best Practices im Sicherheitsbereich, um Angreifern den Zugriff zu Ihrem Netzwerk zu erschweren, ihre Reichweite und die horizontale Beweglichkeit einzugrenzen und um bösartige Aktivitäten zu erkennen. Hier sind einige der besten Strategien:

- Weisen Sie Berechtigungen strikt nach dem Prinzip der geringsten Privilegien zu.
- Verwenden Sie ein mehrschichtiges Sicherheitsmodell, um privilegierte Benutzer von normalen Unternehmensbenutzern zu trennen, wie etwa die Enhanced Security Administrative Environment (ESAE) von Microsoft, die oft auch als Red-Forest-Modell bezeichnet wird.
- Verbieten Sie die Ausführung von nicht vertrauenswürdigem Code.
- Setzen Sie keine veraltete Software ein und installieren Sie die neuesten Patches.
- Überwachen Sie Änderungen in Ihrer Umgebung und verwenden Sie Tools, um Änderungen an den wichtigsten Objekten zu verhindern, wie etwa an Gruppen mit den höchsten Privilegien.
- Überwachen Sie Konfigurations- und andere Systemänderungen aufmerksam auf ungewöhnliche Vorgänge, zum Beispiel auf Befehle, die Bootpartitionen manipulieren oder Systeme zerstören können.
- Überwachen Sie die Aktivitäten der Benutzer, insbesondere für privilegierte Konten. Verwenden Sie idealerweise ein Tool, das eine Baseline der normalen Aktivitäten erstellt, nach Abweichungen sucht und sie kontextgebunden analysiert, um Warnungsermüdung vorzubeugen und gleichzeitig echte Bedrohungen zu erkennen.
- Automatisieren Sie Ihre Reaktion. Moderne Angriffe erfolgen innerhalb von Sekunden. Geben Sie sich nicht mit einem Dashboard in Ihrem Sicherheitscenter zufrieden, denn in der Zeit, die ein Mensch benötigt, um ein Problem zu erkennen, zu analysieren und Gegenmaßnahmen einzuleiten, ist der Schaden schon angerichtet. Daher ist es entscheidend, dass Sie Ihre Sicherheit automatisieren und orchestrieren.

NOTFALLWIEDERHERSTELLUNGS-STRATEGIEN

Mehrschichtige und leistungsstarke Schutz- und Erkennungsstrategien sind zwar wichtig, aber bei Weitem nicht ausreichend. Bei vielen der oben beschriebenen Angriffen wurden die Opfer zurecht dafür kritisiert, dass Sicherheitsgrundlagen nicht beachtet wurden. Zum Zeitpunkt des NotPetya-Angriffs im Jahr 2017 lief auf einem Teil der Maersk-Server beispielsweise noch Windows 2000, dessen Support von Microsoft im Jahr 2010 eingestellt wurde. Außerdem hat die unzureichende Segmentierung des Maersk-Netzwerks dazu beigetragen,

Robuste Schutz- und Erkennungstechniken sind wichtig, aber nicht ausreichend. Sie brauchen auch eine umfassende Notfall-Wiederherstellungs-strategie.

Wenn Sie einem katastrophalen Angriff zum Opfer fallen und nur native Tools zur Verfügung haben, müssen Sie sich auf einen schwierigen, fehleranfälligen und langwierigen Wiederherstellungs-prozess für die Gesamtstruktur vorbereiten.

dass sich die Malware mühelos von ihrem Ausgangspunkt auf das gesamte Netzwerk ausbreiten konnte.

Dabei dürfen wir jedoch nicht vergessen, dass Maersk an der ursprünglichen Infektion keine Schuld traf. Die Malware wurde über eine standardisierte Steuer- und Buchhaltungssoftware ausgeliefert, die in praktisch jedem Unternehmen in der Ukraine eingesetzt wird. Bei diesem Angriff erlitten zahlreiche Unternehmen gravierende Schäden. Viele dieser Unternehmen waren, wie auch Maersk, nicht die beabsichtigten Ziele des Angriffs, sondern lediglich Kollateralschäden.

Die Lektion ist klar: Selbst wenn Ihr Unternehmen keine offensichtlichen Feinde hat und Sie sämtliche von Experten empfohlenen Sicherheitspraktiken beachten, besteht keine Garantie, dass Sie vor zerstörerischen Angriffen geschützt sind. Daher ist eine getestete und erprobte Notfall-Wiederherstellungsstrategie unverzichtbar.

Maersk hatte keine solche Strategie. Das Unternehmen wurde nur durch einen glücklichen Zufall gerettet. Als NotPetya sämtliche 150 Domänencontroller vom Netz genommen hatte, konnte niemand eine Sicherung finden. Ohne die Möglichkeit, die DCs wiederherzustellen, war das Unternehmen völlig hilflos. Dank eines lokalen Stromausfalls war jedoch ein einsamer Domänencontroller in Ghana während des Angriffs nicht am Netz und erwies sich als Rettungsanker für das Unternehmen. Leider war die Bandbreite in der Niederlassung in Ghana so gering, dass der Upload der DC-Daten Tage gedauert hätte. Niemand vor Ort hatte ein britisches Visum, daher musste das Wiederherstellungsteam eine Art Staffellauf veranstalten, um den kostbaren Computer in die britische Unternehmenszentrale zu bringen. Letztlich konnten sie den Computer jedoch verwenden, um die anderen DCs neu aufzusetzen.

Leider verlassen sich zu viele Unternehmen auf solche „Strategien“ für die Notfallwiederherstellung und gehen damit große Risiken ein. Wie wir gesehen haben, wäre der Angriff auf VFEmail beinahe das Ende des Unternehmens gewesen, das nur dank einiger Sicherungsserver überlebt hat, die gerettet werden konnten. Dieser Fall ist besonders ironisch, da der Dienst in der Folge des ILoveYou-Virus eingerichtet wurde, das sich 2001 per E-Mail verbreitete, und die Erkennung von Spam und Malware war eines der wichtigsten Verkaufsargumente. Er ist dazu auch besonders tragisch, da VFEmail im Lauf der Jahre mehreren lähmenden DDoS-Angriffen zum Opfer gefallen ist, diese jedoch scheinbar nicht ernst genug genommen hat.

Native Tools

Wenn Sie einem katastrophalen Angriff zum Opfer fallen und nur native Tools zur Verfügung haben, müssen Sie sich auf einen schwierigen, fehleranfälligen und langwierigen Wiederherstellungsprozess für die Gesamtstruktur vorbereiten.

AD-Gesamtstrukturen sind komplex und umfassen zahlreiche Verbindungen zwischen DCs. Ihre Wiederherstellung ist daher besonders aufwändig. Dazu gehören unter anderem die folgenden Aktivitäten:

- Wiederaufbau der AD-Dienste
- Bereinigung von Metadaten
- Wiederherstellung von Vertrauensbeziehungen
- Zurücksetzen von Konten
- Neustart der Replikation

All diese Aufgaben umfassen komplexe Vorgänge, die korrekt ausgeführt werden müssen. Vergessene oder vertauschte Schritte können dazu führen, dass der gesamte Prozess fehlschlägt. Es ist keine beneidenswerte Aufgabe, eine Gesamtstruktur nur mit nativen Tools unter dem Stress eines katastrophalen Ausfalls manuell und mit der Geschäftsleitung im Nacken wiederherzustellen.

Überzeugen Sie sich selbst davon und sehen Sie sich die Microsoft-Wiederherstellungsanleitung für Active Directory-Gesamtstrukturen an. Diese Anleitung dient als Vorlage für die Wiederherstellung einer Active Directory-Gesamtstruktur, wenn ein systemweiter Ausfall dazu geführt hat, dass sämtliche DCs in der Gesamtstruktur außer Betrieb sind.[2] Hier ist eine Übersicht über die wichtigsten Schritte, wenn eine Wiederherstellung der Gesamtstruktur unvermeidlich ist:

1. **Bestimmen der Vorgehensweise beim Wiederherstellen -** Als Vorbereitung für die Wiederherstellung empfiehlt Microsoft, zunächst den aktuellen Aufbau der Gesamtstruktur und die Funktionen der einzelnen DCs zu ermitteln, zu entscheiden, welcher DC für die einzelnen Domänen wiederhergestellt wird, und sicherzustellen, dass alle beschreibbaren DCs vom Netz genommen werden.

2 Sie finden den Microsoft-Leitfaden zur Wiederherstellung der Active Directory-Gesamtstruktur unter https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide.

Laut der Schätzung von Microsoft dauert allein die Lektüre dieses Vorbereitungsschritts 12 Minuten. Die Beschreibung der einzelnen Teilschritte umfasst je mindestens eine Seite.

2. **Erste Wiederherstellung ausführen (ein DC pro Domäne) -** Grob gesagt besteht dieser Schritt darin, den ersten beschreibbaren DC in jeder Domäne wiederherzustellen, die wiederhergestellten beschreibbaren DCs mit dem Netzwerk zu verbinden und den globalen Katalog zu einem DC in der Gesamtstruktur-Stammdomäne hinzuzufügen.

   Allein der erste Schritt - die Wiederherstellung des ersten DC - umfasst 13 separate Teilschritte, zum Teil jeweils mit mehrteiligen Prozeduren, die von Microsoft separat dokumentiert werden. Beispielsweise müssen Sie ein isoliertes Netzwerk erstellen, Betriebsmaster-Rollen übernehmen, den Wert des verfügbaren RID-Pools erhöhen und die AD-Metadaten der DCs entfernen, die nicht aus einer Sicherung wiederhergestellt wurden.

3. **Erneutes Bereitstellen der restlichen DCs in der Gesamtstruktur -** Sobald Sie eine stabile Gesamtstruktur mit einem DC pro Domäne und einem globalen Katalog haben, können Sie endlich damit beginnen, die restlichen DCs in der Gesamtstruktur bereitzustellen, indem Sie AD DS installieren.

4. **Bereinigung -** Nachdem die Gesamtstruktur wiederhergestellt wurde, müssen Sie dafür sorgen, dass die Benutzer und Geschäftsanwendungen wieder einsatzbereit sind. Unter anderem müssen Sie die Namensauflösung (DNS) neu konfigurieren und herausfinden, welche Änderungen zwischen dem Datum der Sicherung und dem Ausfall vorgenommen wurden und diese Änderungen erneut anwenden.

Diese Schritte sind nicht nur komplex und extrem anfällig für menschliche Fehler, sondern nehmen auch beträchtliche Zeit in Anspruch. Sogar Microsoft räumt ein, dass „die Geschwindigkeit der Wiederherstellung nicht der primäre Zweck dieses Handbuchs ist“. In den begleitenden FAQ wird angemerkt, dass ein Großteil der Wiederherstellung der Gesamtstruktur mit Befehlszeilentools ausgeführt werden kann und Sie daher Skripts schreiben können, um Teile der Wiederherstellung zu automatisieren. Microsoft warnt jedoch auch, dass diese Skripts vor dem Einsatz bei einer tatsächlichen Wiederherstellung gründlich getestet und bei allen Änderungen an der AD-Umgebung aktualisiert werden müssen, zum Beispiel wenn Sie neue Domänen oder DCs hinzufügen oder eine neue Version von Active Directory installieren.

Recovery Manager for AD – Disaster Recovery Edition

Glücklicherweise gibt es Tools, mit denen Sie die Wiederherstellung der Gesamtstruktur automatisieren können, um Ihr Unternehmen schneller und mit viel weniger Aufwand und Risiko wieder auf die Beine zu bringen. Quest® Recovery Manager for Active Directory – Disaster Recovery Edition unterstützt Sie bei der Implementierung einer vollständigen Sicherungs- und Wiederherstellungsstrategie, mit dem Sie Ihre komplette AD-Gesamtstruktur nach jeder Art von Katastrophe auf der Objekt- und Attributebene, der Verzeichnisebene und der Betriebssystemebene wiederherstellen können. Mit der automatisierten Wiederherstellungsfunktion können Sie die Wiederherstellungsdauer nach einem AD-Ausfall auf DC-Ebene sogar um bis zu 95 Prozent reduzieren.

Quest On Demand Recovery erweitert Ihre AD-Sicherung und -Wiederherstellung auf der Objekt- und Attributebene in die Cloud, um nicht nur lokale, sondern auch Hybridumgebungen schützen zu können. On Demand Recovery ist eine schnelle und sichere Sicherungs- und Wiederherstellungslösung für Azure AD und Office 365, mit der Sie Einblicke in reine Cloud-Objekte und die über Azure AD Connect synchronisierten Objekte erhalten, differenzierte Berichte für Produktions- und Echtzeitsicherungen ausführen und koordinierte Wiederherstellungen in Ihrem lokalen AD und in Azure AD ausführen können.

FAZIT

Zerstörerische Angriffe sind auf dem Vormarsch, und ihre Auswirkungen können verheerend sein. Jedes Unternehmen ist verwundbar, entweder als direktes Ziel oder als Kollateralschaden. Nach dem verheerenden Angriff auf VFEmail schrieb der CEO und Gründer Rick Romero auf Twitter: „Ich hätte nie gedacht, dass die Früchte meiner Arbeit jemandem so viel bedeuten würden, dass er sie komplett und restlos zerstören würde.“ Machen Sie nicht denselben Fehler.

Senken Sie Ihre Risiken, indem Sie Best Practices im Sicherheitsbereich einführen, um Angriffe abzuwehren, die Reichweite von Hackern einzugrenzen und eine schnelle Erkennung und Reaktion zu garantieren. Die Ratschläge der Sicherheitsexperten und die Beispiele aus der Praxis zeigen eindeutig, dass eine umfassende Notfall-Wiederherstellungsstrategie unverzichtbar ist. Um mehr über Recovery Manager for AD – Disaster Recovery Edition und On Demand Recovery zu erfahren, besuchen Sie quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition und quest.com/products/on-demand-recovery.

Implementieren Sie eine vollständige Sicherungs- und Wiederherstellungs-strategie für Ihre Hybridumgebung mit Quest Recovery Manager for AD und On Demand Recovery

ÜBER QUEST

Quest liefert Softwarelösungen für die ständig im Wandel befindliche Welt der Unternehmens-IT. Wir helfen, die durch Datenexplosion, Cloud-Erweiterung, Hybrid-Rechenzentren, Sicherheitsbedrohungen und gesetzliche Bestimmungen hervorgerufenen Schwierigkeiten zu verringern. Wir sind der globale Anbieter für 130,000 Unternehmen in 100 Ländern, einschließlich 95 % der Fortune 500 und 90 % der Global 1000. Seit 1987 entwickeln wir eine Palette von Lösungen, die aktuell Datenbankverwaltung, Datensicherung, Identitäts- und Zugriffsverwaltung, Microsoft-Plattformverwaltung sowie die Verwaltung vereinheitlichter Endgeräte umfasst. Mit Quest investieren Unternehmen weniger Zeit in die IT-Administration und haben mehr Zeit für geschäftliche Innovationen. Weitere Informationen finden Sie auf www.quest.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:
www.quest.com/de-de/company/contact-us.aspx