Mythen hinterfragen – Sicherheit richtig umsetzen

Es reicht nicht, teure Sicherheitssoftware einzukaufen und einen externen Penetrationstest zu bestellen. Bei der IT-Sicherheit kommt es auch auf die richtige Implementierung, den adäquaten Betrieb der Produkte und einiges mehr an.

Von Frank Ully

Neben dem passenden Mindset, das ein Schwerpunkt des ersten Teils der Titelgeschichte war, sind weitere Faktoren relevant für die IT-Sicherheit eines Unternehmens: insbesondere der sinnvolle Einsatz von Sicherheitsprodukten und deren fehlerfreie Implementierung, aber auch der richtige Umgang mit Zertifizierungen und Sicherheitstests. Nicht zuletzt gilt es, das Erkennen von Angriffen zu forcieren und nicht alle Mittel und Energie in die Prävention zu stecken. Auch zu diesen Aspekten kursieren viele Halbwahrheiten und Irrtümer, die es zu beleuchten gilt.

„Wir betreiben Compliance und sind deswegen sicher“

PCI DSS für das Verarbeiten von Zahlungsdaten, ISO 27001 für ein Informationssicherheitsmanagementsystem und SOC 2 für Dienstleister sind bewährte Compliancestandards.

Das Einhalten solcher Vorschriften und Konformität nach Checklisten können Grundlagen etablieren und attestieren, ob sie zum Zeitpunkt des Audits eingehalten wurden. Sie helfen, Fahrlässigkeit zu vermeiden. Sicher machen sie per Definition nicht (siehe Abbildung 1). Bei vielen Sicherheitsvorfällen, von denen in der Tagespresse zu lesen ist, war das Unternehmen nach mehreren Compliancestandards zertifiziert.

Eine Frage der Implementierung

Aus der Compliance-Denkschule stammt der Trugschluss „Unsere Daten sind verschlüsselt und deswegen sicher“. Aber: Die Transportverschlüsselung einer Webapplikation über HTTPS schützt nur den Weg von Server oder Proxy zum Browser. Kryptografie garantiert in diesem engen Bereich Vertraulichkeit über den Inhalt der Nachrichten. Sie verheimlicht aber schon nicht mehr die stattfindende Kommunikation, ihre Länge, Dauer oder die Partner.

Irgendwann muss ein Computer verschlüsselte Daten zum Verarbeiten wieder entschlüsseln – außer bei nicht praxisrelevanter homomorpher Verschlüsselung [1]. Malware auf dem Anwendungs- oder dem Datenbankserver oder dem Mobiltelefon eines Benutzers kann die dort verarbeiteten Daten abziehen. Je nach Anwendung und Art der Kryptografie garantiert sie womöglich nicht einmal Integrität oder Authentizität. Die Diskussion über den richtigen Algorithmus, die ausreichende Schlüssellänge und akzeptable Chiffren lenkt oft von anderen wichtigen Baustellen ab. Wenn der AES256-Schlüssel, der die Betriebsgeheimnisse sichert, prominent auf einer öffentlichen Netzwerkfreigabe liegt, hilft all die komplexe Mathematik nicht.

Schlecht umgesetzte Compliance führt zu einem trügerischen Sicherheitsgefühl und wahrscheinlich zu weniger Schutz vor echten Widersachern. Wenn es eine Schwachstelle gibt, werden Hacker sie früher oder später finden und ausnutzen. Vor allem verengt eine starre Compliance-Brille die Sicht der Verteidiger. Diese sollten jedoch immer wie Angreifer denken und deren Sichtweise verstehen. Schließlich schützen Sicherheitsverantwortliche und Admins sich nicht vor einer virtuellen Bedrohung, sondern vor echten menschlichen Gegnern und ihrem kreativen Vorgehen. Verteidiger müssen berücksichtigen, wie Angreifer versuchen, Sicherheitsmaßnahmen zu umschiffen oder deren Angriffsfläche gegen die Organisation zu wenden. Nur dann können sie bewerten, was sicherer macht. Der bereits im ersten Teil der Titelgeschichte zitierte Microsoft-Sicherheitsexperte John Lambert schreibt: „Offense and defense aren’t peers. Defense is offense’s child“ (siehe ix.de/z8uu).

„Wir machen Penetrationstests und wissen, dass wir sicher sind“

Wie sicher eine Organisation ist, kann ein einmaliger Sicherheitstest nicht messen. Er prüft bestimmte Aspekte der Umgebung in definiertem Umfang in einer begrenzten Zeit, etwa eine frisch installierte Webanwendung in der Produktion. Die Anwendung wird abgesegnet – und Kriminelle stehlen Kundendaten von einem vergessenen Testsystem mit einer älteren Softwareversion, das aus dem Internet erreichbar ist und zum Test einer Migrationsfunktion diente. Über den Rest des Netzwerks kann ein punktueller Test ohnehin keine Auskunft geben. Zudem ist eine Sicherheitsanalyse eine Momentaufnahme. Schon einen Tag nach Berichtsversand kann das Unternehmen die Funktion ausrollen, die unsicher implementiert ist.

Bug-Bounty-Programme vergüten freischaffende Kopfgeldjäger mit einer Prä-

mie für eine gefundene Schwachstelle. Sie stehen zumindest großen Organisationen wie Apple oder Microsoft gut zu Gesicht. Bounties belohnen das verantwortungsbewusste Melden, statt die Hacker zu zwielichtigen Schwachstellenbrokern zu treiben. Nur für eine wirkliche Lücke zu bezahlen, hört sich auch für kleinere Organisationen gut an. Doch das Initiieren einer solchen Suche ersetzt kein systematisches Audit. Die Beziehungen zu einzelnen Testern sind nicht so langfristig wie die Zusammenarbeit mit einem Sicherheitsberater – und die eintrudelnden Meldungen wollen bewertet und beantwortet werden.

Ein Test ist ohnehin ineffektiv, wenn das Unternehmen die entdeckten Lücken nicht systematisch verwaltet, bewertet und behebt. Lambert stellt fest: Der Sicherheitstest ist die Diagnose. Seine Befunde sollten nicht als Ausgabe dienen, die man abheftet und als Beleg für ein absolviertes Audit archiviert. Die Verantwortlichen müssen die aufgedeckten Risiken bewerten und als Eingabe für eine kontinuierliche Verbesserung behandeln. Beheben sie die Ursachen nicht, ist das Problem nur vorübergehend überdeckt. Die gemeldete Lücke muss im untersuchten Teil der Anwendung gestopft werden, sie schlummert aber womöglich auch in anderen Funktionen. In ähnlicher Software oder auf verwandten Systemen sollte die Organisation ebenfalls nach ihr jagen.

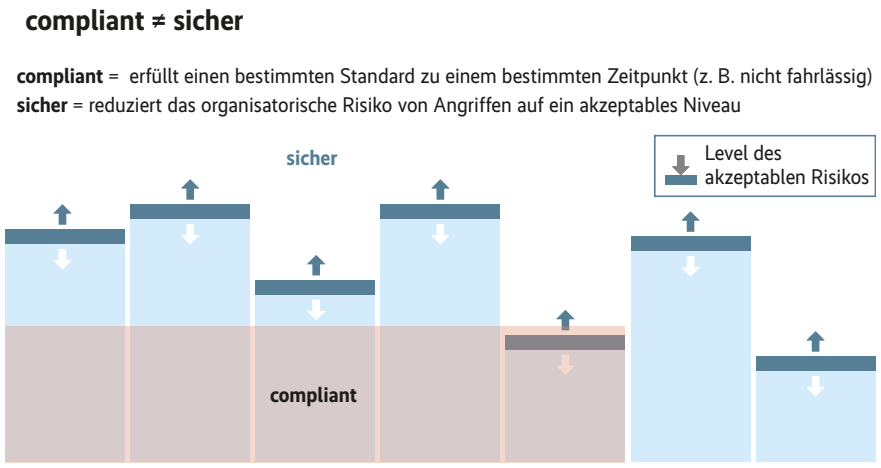
Sicherheitstests lohnen sich. Sie machen auf offensichtliche oder versteckte Risiken aufmerksam. Sie ersetzen aber nicht weitere Maßnahmen und keine Strategie, Richtlinien und Prozesse.

„Uns kommt keine Schadsoftware auf die Rechner, wir haben einen Malware-Scanner“

Malware-Scanner sind ein wichtiger Sicherheitsbaustein. Allerdings kennen Angreifer zahlreiche Methoden und schlüsselfertige Werkzeuge, um von Antivirensoftware zunächst erkannten Schadcode so zu verändern, dass Scanner nicht mehr anschlagen oder zumindest das vom Opfer verwendete Produkt nichts merkt. Selbst wenn die Verschleierungsmethoden der meisten öffentlich verfügbaren Tools von Antivirenherstellern irgendwann teilweise erkannt werden, gibt es bis zu deren Update eine Schutzlücke.

Oft machen es Organisationen den Eindringlingen viel zu leicht, weil Malware-Scanner nur auf Arbeitsplätzen von Endbenutzern laufen. Ein Angriff hat jedoch mehrere Phasen, bei denen die Angreifer sich von System zu System hangeln [2]: vom zunächst kompromittierten Mitarbeiterrechner auf einen Server, von dort zum nächsten Server bis etwa zu einem Domänencontroller. Bei jedem dieser Schritte führen sie verschiedene offensive Werkzeuge aus, die ein Scanner theoretisch erkennen könnte. Sind abseits von Clients keine Scanner installiert, findet die nicht vorhandene Antivirenlösung auf Servern keinen Schadcode. Selbst fortgeschrittene Angreifer machen Fehler oder sind aus Erfahrung nachlässig und verwenden erkennbare Schadsoftware.

Quelle: Microsoft



Auch Microsoft weist in einem Artikel explizit darauf hin, dass compliant nicht automatisch sicher bedeutet (Abb. 1).

Noch immer investieren Unternehmen meist nur in das Verhindern und kaum in das Erkennen möglicher Sicherheitsvorfälle. Bei vielen Angriffsschritten reicht ein Malware-Scanner zur Erkennung vollkommen aus (Abbildung 2), ohne dass man weitere teure Securitytools benötigt oder Ansätze mit aufwendiger Installation und Betrieb wie ein Security Information and Event Management (SIEM) implementiert.

Virenscanner besser nutzen

Bedauerlich ist, wie viele Organisationen ihren Malware-Scanner still die Arbeit verrichten und potenzielle Bedrohungen wegblocken lassen, ohne seine Alarme zentral zu sammeln, in die Protokolle zu sehen und frühzeitig zu reagieren. Frühzeitig bedeutet innerhalb eines Geschäftstages und ist ideal als laufende Übung, bevor ein richtiger Angriff passiert. Da das kaum gemacht wird, können Eindringlinge in einer kompromittierten Umgebung so lange ihre Angriffswerkzeuge verändern, bis sie nicht mehr erkannt und weggelöscht werden.

Für Sicherheitsverantwortliche ist es eine vertane Gelegenheit, wenn sie den Malware-Scanner als ohnehin vorhandene Basislösung nicht richtig nutzen. Jeder einzelne Alarm, auch mit niedriger Priorisierung, kann ein Signal für einen laufenden Einbruch sein und bietet die Chance, ihn zu erkennen, zu stoppen und das Schlimmste zu verhindern. Oft enthüllen Vorfalluntersuchungen nachträglich: Die ersten Anzeichen für den Angriff standen in den Protokollen des Malware-Scanners.

Schadsoftwareklassifizierungen der Hersteller sind teilweise unverständlich. Systemverwaltern hilft das „Antivirus

iX-TRACT

- Die richtige Einstellung bei der Verteidigung gegen Angriffe ist zwar schon viel wert, ohne planvolle Maßnahmen, ausgewählte Tools und gute Erkennungsmechanismen geht es dennoch nicht.
- Oft ist es besser, nur wenige sinnvolle Sicherheitssysteme einzusetzen und diese in ihrem Potenzial voll auszuschöpfen, als bei zu vielen Tools den Überblick zu verlieren.
- Viele Maßnahmen sind schon für wenig Geld oder kostenlos zu haben.
- Gerade kleine Unternehmen können entsprechende Angebote von Behörden und Organisationen in Anspruch nehmen.

Event Analysis Cheat Sheet“ (Abbildung 3; siehe ix.de/z8uu), Meldungen einzuordnen und etwa bei den Werkzeugen Cobalt Strike, Mimikatz oder Seatbelt in der Erkennungsnachricht Alarmstufe Rot auszulösen.

Allerdings müssen sich Verteidiger darauf einrichten, dass Angreifer zum dauerhaften Zugang in eine bereits übernommene Umgebung zunehmend legitime Fernwartungssoftware wie AnyDesk oder TeamViewer verwenden, die nicht als Schadsoftware erkannt wird. Davor warnte jüngst die amerikanische Cybersecurity-Behörde CISA. In ihrer Meldung gibt sie weitere Hinweise, wie damit umzugehen ist. Dateiformate, die modernen Angreifern zum initialen Zugriff dienen, wie Windows-Verknüpfungen (.lnk), OneNote-Notizbücher (.one) oder CD-Abbilder (.iso) unterstützen manche Scanner zudem noch nicht gut (Details siehe ix.de/z8uu).

„Sicherheit entsteht ausschließlich durch Prävention“

Organisationen investieren oft nur in das Verhindern von Sicherheitsvorfällen und geben den größten Teil ihres Budgets für im Kern präventive Maßnahmen aus – für Patch- und Identitätsmanagement, Firewalls und Webfilter, Schwachstellenscans und Pentests. Das Erkennen möglicher Vorfälle ist bestenfalls ein Nachgedanke, wenig Ressourcen fließen in entsprechende Ansätze und Prozesse. An Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) [3] oder zentrale Logauswertung ist meist nicht zu denken. Vorbeugen ist ideal, Erkennen von Angriffen ein Muss – irgendwann wird der Schutz versagen. Mögliche Werkzeuge sind ein SIEM (Security Information and Event Management) oder Produkte, die sich auf Erkennung (Detection) spezialisiert haben.

Geschützte Umgebungen legen die Messlatte höher und verlangen den Angreifern mehr Zeit und aufwendigeres Vorgehen ab, um an ihr Ziel zu kommen. Ein ungesichertes Active Directory (AD) ist im schlimmsten Fall über den Feierabend automatisiert komplett verschlüsselt, wie der DFIR-Bericht im vorangegangenen Artikel zeigt (siehe Seite 44). Eine gehärtete Umgebung bremst Erpresser: Sie müssen sich selbst vor den Bildschirm setzen und händisch nach Lücken suchen. Das verschafft den Verteidigern Gelegenheit, den laufenden Einbruch zu entdecken – in realistischen Zeitspannen. Prävention schafft Freiraum, um Sicherheitsvorfälle zu erkennen. Viele Eintrittswege wurden versperrt und es hagelt nicht mehr Warnungen über hoffnungslos veraltete Systeme, in deren Flut Angriffsversuche untergehen.

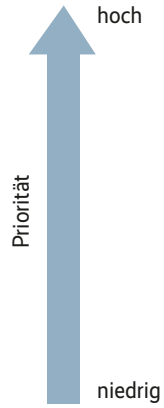
Mit Honig fängt man Kriminelle

Einen niedrigschwelligen Einstieg in die Erkennung bieten intern platzierte Honigtöpfe. Weil sie kaum Fehlalarme auslösen, hilft das schon Organisationen mit niedrigem Sicherheitsniveau.

Um komplett sicher zu sein, müssten Verteidiger sämtliche Schwachstellen stopfen. Angreifern dagegen reicht für jeden Schritt ihrer Attacke eine Lücke, die sie erfolgreich ausnutzen. Deception, also Täuschung, stellt diesen Ansatz auf den Kopf. Sie wendet die bei Angreifern beliebte Taktik gegen sie selbst, sich etwa bei einer Phishing-E-Mail als jemand anders auszugeben. Täuschung verfolgt den Ansatz, Eindringlinge zu entdecken, indem man sie mit falschen Fährten wie scheinbar echten Zugangsdaten, Diensten, Benutzern, Geräten oder Dokumenten in die Falle lockt. Da sie gefälschte nicht von echten Daten unterscheiden können, werden sie versuchen, sie zu verwenden, und lösen einen Alarm aus.

Mit Täuschung müssen Einbrecher jeden aufgespannten Stolperdraht umgehen, um nicht entdeckt zu werden. Verteidiger müssen nur eine der Alarmglocken hören. Kein legitimer Benutzer sollte auf ein Honigtopfsystem zugreifen oder die als Falle ausgelegten Zugangsdaten verwenden. Jede Interaktion damit ist mindestens verdächtig, im schlimmsten Fall bösartig. Selbst entdeckte Täuschungsversuche sind nicht nutzlos, sondern bremsen Angreifer weiter aus. Sie können den gesammelten Daten nicht mehr vorbehaltlos vertrauen und müssen sich bei jedem Schritt fragen, ob sie womöglich erneut in eine

Log-Quelle	Volumen[11]	IoC-Abgleich	Threat Hunting	Protokollfunktion[9]	APT-Erkennung[10]
Antivirus	niedrig	–	++[3]	+	+++
Windows und Sysmon	mittel[8]	++[1]	+++[4]	++	++
Proxy	mittel	++[2]	+[5]	++	+
NIDS/NSM[7]	mittel	+[2]	+	+	+
DNS	hoch	++[2]	+[5]	+	+
Mail[6]	mittel	+	–	+	–
Firewall	hoch	+[2]	–	++	–
Linux (auditd)	mittel	–	+	+	–



1 Dateihashwerte (MD5, SHA1, SHA256)
2 IP-Adressen oder Domänennamen von Command-and-Control-Servern
3 siehe „Antivirus Event Analysis Cheat Sheet“
4 Sigma kann sehr hilfreich sein
5 Muster (URL, Hostname), verdächtige Top-Level-Domains
6 keine persönliche Erfahrung mit dieser Protokollquelle, aber von anderen sehr empfohlen
7 Suricata, Zeek oder Ähnliches
8 hängt hauptsächlich von der Überwachungsrichtlinie (Microsoft Baseline verwenden) und der Sysmon-Konfiguration ab
9 Nützlichkeit beim Rekonstruieren von Ereignissen
10 Wie nützlich sind diese Protokolle bei der Erkennung anhaltender Bedrohungen (Aufklärung, Hintertüren, laterale Bewerbung)?
11 hängt von Audit-Richtlinien und Filtern ab (Faustregel)

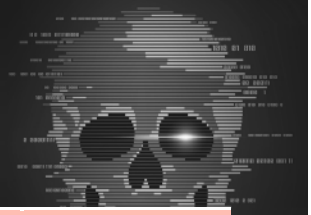
Quelle: Florian Roth, Maturity Model of Security Disciplines

Antivirusprodukte eignen sich besonders gut zum Erkennen von Angreifern (APT Detection) (Abb. 2).

Quelle: Nextron Systems

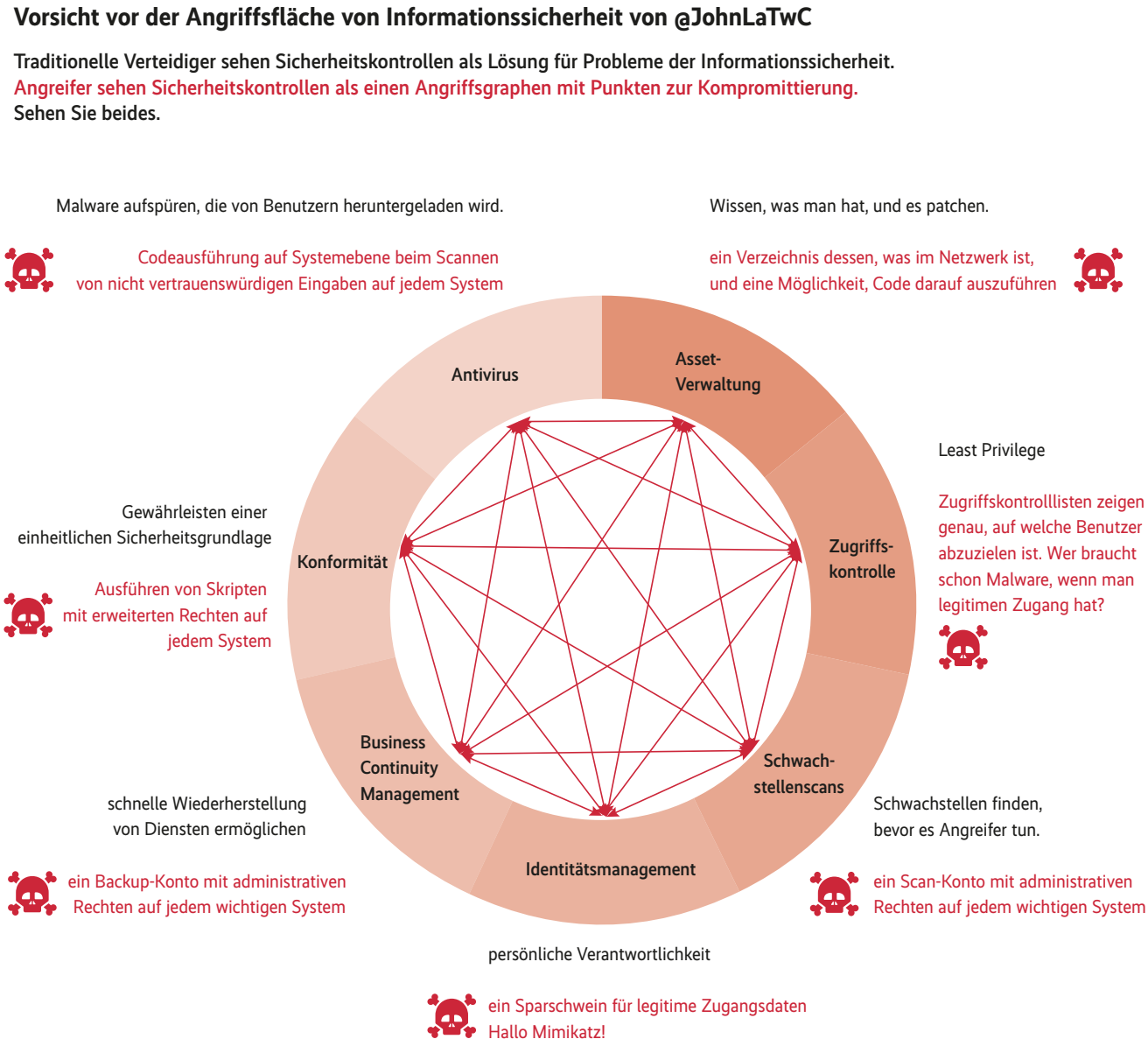
Antivirus Event Analysis Cheat Sheet

Version 1.12.0, Florian Roth @cyb3rops



Attribute	Less Relevant	Relevant	Highly Relevant		
Virus Type	Adware Clickjacking Crypto FakeAV HTML Iframe Joke Keygen Tool-Nmap	Agent Backdoor Clearlogs Creds Crypto Exploit JS LNK Malware Miner NetTool PassView PowerShell PS RemAdm Scan Stealer Tool-Netcat Trojan Wacatac	Adfind ASP/BackDoor ATK/ Backdoor.ASP Backdoor.Cobalt Backdoor.JSP Backdoor.PHP Blackworm Brutel BruteR Chopper Cobalt COBEACON Cometer CRYPTES Cryptor Cryptor Destructor DumpCreds Exploit.Script.CVE Filecoder FRP. FastReverseProxy	GrandCrab HackTool HKTL HTool Impacket IISExchgSpawnCMD JSP/BackDoor Keylogger Koadic Krypt Lazagne Locker Metasploit Meterpreter MeteTool Mimikatz Mpreter Nighthawk Packed.Generic.347 PentestPowerShell Phobos PHP/BackDoor Potato	PowerSploit PowerSSH PshlSpy PSWTool PWCrack PWDump PWS. PWSX Ransom Razy Rozena Ryuk Ryzerlo Sbelt Seatbelt SecurityTool SharpDump Sliver Swrort Tescrypt TeslaCrypt Valyria Webshell
Location	Temp Internet Files Removable Drive (E:, F:, …) All other folders	C:\Temp $Recycle.bin C:\ProgramData C:\Users\Public C:\Users\All Users AppData\Local\Temp AppData\Roaming\Temp C:\Windows\Temp	C:\Windows\System32 C:\Windows C:\ \\Client\[A-Z]$ (remote session client drive) \\tsclient\<drive> C:\PerfLogs \FrontEnd\HttpProxy\owa\auth\ \inetpub\wwwroot\aspnet_client\ *$ (execution on remote host) Other directories that are writable for Administrators only		
User Context		Standard User	Administrative Account Service Account		
System	File Server Ticket System	Workstation Email Server Other Server Type	Domain Controller Print Server DMZ Server Jump Server Admin Workstation Application Proxy Connector		
Form / Type	Common Archive (ZIP)	Not Archived / Extracted, Uncommon Archive (RAR, 7z, encrypted Archive)	File Extensions: .ASP .ASPX .BAT .CHM .HTA .JSP .JSPX .JAR .LNK .PHP .PS1 .SCF .TXT .VBS .WAR .WSF .WSH .XML .CS .JPG .JPEG .GIF .PNG .CS .CAB .ISO .JNLP .IMG .DIAGCAB .APPX .DMG .ONE		
Time		Regular Work Hours	Outside Regular Work Hours, Public Holidays		
Google Search (File Name)		Well-known Malware (e.g., mssecsvc.exe) or no result at all	APT related file mentioned in report		
Virustotal (Requires Hash / Sample)	**Notes >** "Probably harmless", "Microsoft software catalogue" **Tags >** trusted, known-distributor, zero-filled **File Size >** Less than 16 byte (most likely an empty file, error page etc.)	**Comments >** Negative user comments **Tags >** url-pattern, auto-open, obfuscated, via-tor, lnk, invalid-signature **File names >** *.virus **Packers identified >** Uncommon Packers like: PECompact, VMProtect, Telock, Petite, WinUnpack, ASProtect **Suspicious combinations >** e.g. UPX, RARSFX and Microsoft Copyright	**File Detail >** Revoked certificate **Tags >** spreader, dropper, cve-20*, exploit, revoked-cert, trojan, yoda*, hiding-window **Packers identified >** Rare Packers like: Themida, Enigma, ApLib, Tasm, ExeCryptor, MPRESS, ConfuserEx **Comments>** THOR APT Scanner: "Hacktools", "Threat Groups", "Webshell", "Cobalt Strike", "Empire", "Mimikatz", "Veil", "Privilege Escalation", "Password Dumper", "Koadic", "Elevation", "Winnti"		

Übersichtlicher als Herstellerinformationen: Ein Cheat Sheet kann dabei helfen, Antivirusmeldungen zu bewerten (Abb. 3).



Die Angriffsfläche von Informationssicherheit nach John Lambert: Verteidiger sollten auf sie auch mit den Augen der Angreifer schauen (Abb. 4).

Falle der Verteidiger tappen. Ein früherer iX-Artikel liefert mehr Hintergründe und Ideen zu Deception [4].

„Bei uns bleiben keine Malware und kein Angreifer unentdeckt, wir verwenden ein EDR“

Mit EDR und XDR drängen neuere Techniken auf den Massenmarkt, die über kompromittierte Systeme alarmieren, weil sie auf den Endpunkten bösartiges Verhalten erkennen. Fortgeschrittene Angreifer haben sich daran angepasst und können EDR-Anwendungen mit Aufwand, Experimentieren und Fantasie aushebeln. Sicherheitsforscher konnten in einer Studie alle untersuchten EDRs umgehen (siehe ix.de/z8uu). Die erwähnten kommerziellen Fernwartungswerkzeuge sind dafür eine Möglichkeit. Eine andere sind neuere Angriffstechniken wie DLL Sideloading, bei dem legitimen Anwendungen der Schadcode als Bibliothek untergeschoben wird. EDR-Hersteller vermeiden, zu viele falsch positive Alarme auszulösen. Dazu bauen sie Ausnahmen in ihre Erkennungsregeln ein, weil sie sonst viel harmlose Software als verdächtig einstufen. Linux-Server unterstützt und überwacht eine Endpunktlösung womöglich gar nicht; Eindringlinge nisten sich dort gerne ein und haben von da aus häufig Zugriff auf die verbundene Windows-Domäne.

An dieser Stelle lohnt ein erneuter Verweis auf Lambert, der in einem Diagramm warnt (Abbildung 4): Gut gemeinte Maßnahmen zum Steigern der Informationssicherheit können neue, tiefe Lücken reißen und die Angriffsfläche vergrößern, wenn man sie unbedacht einsetzt. Eine EDR-Software auf jedem Arbeitsplatz, die sich aus der Cloud-Konsole des Anbieters heraus von zahlreichen Supportmitarbeitern zur Vorfalluntersuchung fernsteuern lässt, eröffnet Angreifern ungewollt weitere Wege zum Übernehmen des AD. Etwa, wenn die Konsole die Kontrolle der Rechner von Domänenadministratoren ermöglicht. Überdies können in Sicherheitstools ähnlich wie in anderer Software patchbare Lücken klaffen.

„Dieses Sicherheitstool mit KI und Blockchain-Anschluss wird uns schützen“

Manche Verantwortliche und Entscheider glauben den Einflüsterungen der Si-

cherheitsindustrie, ihr neuestes Cloud-Produkt wäre absolut unschlagbar. Einerseits stimmt das wie oben beschrieben nicht. Andererseits verleitet das Gefühl, unter der schützenden Hand künstlicher Intelligenz aus der Analysewolke zu stehen, zu riskantem Verhalten: etwa zu unbedachtem Öffnen eines Anhangs im Glauben, die Kontrollen würden greifen.

Einzelne Tools können immer nur Teil einer, wie es so schön heißt, ganzheitlichen Sicherheitsstrategie sein, die neben Technik auch Prozesse und Menschen umfasst. Vor allem wollen teuer eingekaufte Werkzeuge mit bunten managementgerechten Dashboards eingerichtet, überwacht, gewartet und sinnvoll mit anderen Maßnahmen verbunden werden. Mitarbeiter müssen dafür geschult werden und zur Auswahl, Einführung und hinterher im Tagesgeschäft Zeit haben. Wie am Beispiel der Malware-Scanner beschrieben, ist es wirksamer, wenige Werkzeuge effizient einzusetzen, um den Aufwand für Angreifer zu erhöhen, statt viele Tools schlecht eingeführt und kaum gepflegt aneinanderzureihen. Das treibt nur interne Kosten in die Höhe und führt bei Mitarbeitern zur inneren Kündigung.

Sicherheit ist ein Prozess, kein Produkt. Vor allem nicht ein einziges Produkt. Im Sinne einer Verteidigung in der Tiefe sollte man Sicherheitsmaßnahmen auf verschiedenen Ebenen kombinieren [5]. Wenn eine Schutzschicht versagt, darf nicht gleich die gesamte Umgebung fallen. Manche Branchenkenner prognostizieren, ein „Security Tools Crash“ (siehe ix.de/z8uu) stehe bevor: Zu viele Anbieter tummeln sich auf diesem Markt, Sicherheitsteams fordern weniger Werkzeugverhau und manches Budget schrumpft wegen der wirtschaftlichen Lage.

„Wir sammeln Protokolle, betreiben ein SOC und werden Angreifer sofort erkennen“

Eine Organisation sammelt wie empfohlen sämtliche relevanten Logs von allen inventarisierten Systemen ein, speist sie in eine zentrale Plattform [6] – und wird von einer Erpresserbande kaputtverschlüsselt. Wie konnte das passieren? Das Anhäufen von Protokolldaten führt noch nicht zu Erkennung. Erst Überwachungsregeln und Mechanismen, die über ungewöhnliche oder verdächtige Vorgänge alarmieren, können Angriffe aufspüren. Dabei helfen die öffentlichen und kostenfreien Regeln des Sigma-Projekts (siehe ix.de/z8uu und [7]).

Zudem wuchert in typischen Netzwerken eine Schatten-IT, die kaum gesichert ist und keine Protokolldaten an ein SIEM sendet. Der Vorteil eines Angreifers ist der Unterschied zwischen dem, was die Organisation hat, und dem, was sie verwaltet. Misstrauisch machen sollten ausbleibende Logeinträge eines bekannten Systems oder null Alarme in Sicherheitsprodukten wie Malware-Scannern, SIEM oder EDR. Eindringlinge könnten das Einspeisen neuer Daten in den bereits gekaperten Systemen abgeklemmt oder die zentralen Sammelstellen sabotiert haben.

Selbst wenn ein Monitoring eingerichtet ist, auf das ein internes oder externes Security Operations Center (SOC) [8] ein wachsames Auge hat, sind einlaufende Meldungen größtenteils falsche Alarme. Das führt zu einer gewissen Müdigkeit der Besatzung. So kommt es leicht, dass unerfahrene Analysten im Stress einen Alarm

über die erkannte Schaddatei eicar.exe unbedacht als falschen Verdacht wegklicken. Denn so heißt auch eine normierte Malware-Scanner-Testdatei. Die Software ist aber wirklich bösartig und die Datei absichtlich irreführend benannt. Florian Roth hat auf Twitter weitere Namen für Malware-Dateien gesammelt, die Analysten täuschen können (siehe ix.de/z8uu).

Gerade wenn eine Organisation sich gut gewappnet fühlt oder sogar Stolperfallen gelegt hat, sollte sie nicht der Fehlwahrnehmung erliegen, ihre Mitarbeiter stellten einen Angriff sofort fest. In Europa dauert es im Mittel eineinhalb Monate, bis das Opfer den Einbruch entdeckt. Der im vorigen Jahr erschienene FireEye MTrends Report 2022 analysiert weitere Details (siehe ix.de/z8uu). Im Einzelfall dauert es oft länger: Die Hotelkette Marriott bemerkte den munter sprudelnden Abfluss von Gästedaten erst nach vier Jahren.

„Wir wissen, wie wir im Notfall reagieren“

Meldet ein Malware-Scanner, ein anderer Erkennungsmechanismus oder das SOC den bestätigten Fund einer Schadsoftware zum Diebstahl von Zugangsdaten, könnten Verteidiger sich über diesen Erfolg auf die Schulter klopfen. Aber wie gelangte die Malware dorthin? Irgendjemand hatte die Rechte, sie dort abzulegen und auszuführen. Schon ist man mitten in der Vorfallsbewältigung.

Der schließlich bemerkte Alarm oder, im ungünstigsten Fall, das Erpresserschreiben ist der Zeitpunkt, zu dem Opfer auf das Verbrechen aufmerksam werden. Zuvor haben sich die Täter Tage oder Wochen im Netzwerk breitgemacht. Je länger sie unbemerkt auf die Systeme zugreifen konnten, desto weiter konnten sie sich vorarbeiten, Backups löschen oder Hintertüren einrichten.

Einige Unternehmen geben Unsummen für Detektionstools aus, denken aber kaum an die Reaktion. Erkennen ohne angemessenes Reagieren ist von geringem Wert. Wichtig sind das Entwickeln und Üben eines Prozesses für das Behandeln von Vorfällen, wenn noch kein Incident-Response-Prozess etabliert ist [9]. Den Schaden vergrößern vor allem Aktionismus oder der nur vermeintliche Hinauswurf der Eindringlinge, die über die Hintertür wiederkommen.

Nicht trainierte Notfallpläne aus der Schublade lindern den Stress eines Vorfalls nur wenig. Sie lesen sich womöglich auf dem Papier gut, überstehen in der Praxis aber nicht die Feuertaufe. Das Reagieren auf Sicherheitsvorfälle müssen Verteidiger regelmäßig und so realistisch wie möglich proben. Übungen, bei denen Backups versuchsweise wiederhergestellt werden, können aufdecken, dass wichtige Daten zuletzt gar nicht gesichert wurden. Allein davon auszugehen, man werde im Notfall alle erreichen, ist ein Trugschluss. In der Realität sitzen relevante Mitarbeiter in Meetings, sind auf Geschäftsreise oder im Urlaub oder schon mit dem Tagesgeschäft überlastet. Den ausgedruckten Ablaufplänen sollte zumindest die Telefonnummer eines Incident-Response-Dienstleisters beiliegen, der helfen kann, wenn eine Firma selbst überfordert ist.

„Wir können nichts gegen bösartige Hacker tun“

Vor allem KMU werfen leicht angesichts der Bedrohungslage die Arme in die Luft. Sie glauben, sich mehr als eine Firewall und das obligatorische Antivirus sowieso nicht leisten zu können. Sicherheit ist aber kein binärer Zustand von gehackt oder nicht gehackt (siehe ix.de/z8uu).

Die beschriebenen Sicherheitsirrtümer ergänzt der kurzweilige YouTube-Vortrag von Keith Palmgren. Er hat im Lauf seiner langen Karriere vierzehn „absolute Wahrheiten“ über Informationssicherheit zusammengetragen, beginnend mit „Es gibt keine Sicherheit, nur unterschiedliche Grade von Unsicherheit“. Zum Nachdenken regen die zehn unveränderlichen Gesetze der Sicherheit an, von Microsoft recht prominent aufgestellt in der Einführung zu seinen bewährten Methoden für Sicherheit (beides zu finden über ix.de/z8uu).

Im Februar 2023 erschien das Taschenbuch „Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls That Derail Us“ des renommierten Sicherheitsforschers Eugene Spafford. Zusammen mit seinen beiden Co-Autoren Leigh Metcalf und Josiah Dykstra beschreibt er systematisch, quellensatt und humorvoll Hunderte Irrtümer von Anwendern, Führungskräften und Sicherheitsexperten und wie man sie vermeidet. Die Verfasser schildern, wie Analogien wie die des „schwächsten Glieds in der Kette“ zu Fehlschlüssen führen. In der Onlinebibliothek von O’Reilly, die zeitlich begrenzt getestet werden kann, schmökern Interessierte kostenfrei in der E-Book-Version (siehe ix.de/z8uu).

Viele Maßnahmen – Detektion durch effizient genutzte Malware-Scanner oder Honigtöpfe – müssen gar nicht viel Geld kosten, wie in diesem Artikel skizziert. Neben dem BSI bieten andere Cybersicherheitsagenturen wie ENISA und CISA für kleine und mittelständische Unternehmen nützliche Handreichungen. Die CISA pflegt außerdem eine Liste mit kostenfreien Diensten und Werkzeugen, die helfen, das Risiko eines Vorfalls zu verringern, einen Einbruch zu erkennen und darauf zu reagieren (siehe ix.de/z8uu). Es gibt also keine Ausreden mehr, nicht mit der Umsetzung von IT-Sicherheit im Unternehmen anzufangen. (ur@ix.de)

Quellen

[1] Mirko Ross; Luftsicherheit; Sichere Verschlüsselung bei kollaborativer Datenverarbeitung; iX 8/2021, S. 90

[2] Frank Ully; Fette Beute; Passwörter und Hashes – wie Angreifer die Domäne kompromittieren; iX 11/2020, S. 94

[3] Konstantin Bücheler, Martin Hartmann, Alain Rödel, Stefan Strobel; Auf dem Radar; Endpoint Detection and Response: Gefahren schnell erkennen und reagieren; iX 11/2021, S. 52

[4] David Fuhr; Null Vertrauen: Zero-Day und Zero Trust; iX 12/2022, S. 82

[5] Michael Friedrich; Logging-Plattformen im Vergleich; iX 9/2022, S. 58

[6] Fabian Murer, Gregor Wegberg; Aufgespürt; AD-Sicherheit: Angriffsspuren analysieren; iX 1/2022, S. 124

[7] Oliver Schonschek; SOC: optimierte Security nicht nur für die Kleinen; iX 10/2022, S. 130

[8] Uwe Grams, Yannik Wiederhöft; Raus aus der Panik; Nach dem Angriff: die Arbeit eines Incident-Response-Teams; iX 3/2022, S. 50

[9] Die im Text erwähnten Artikel, Blogbeiträge, Tools und Hilfestellungen sind über ix.de/z8uu zu finden.

FRANK ULLY

ist Head of Research der Oneconsult Deutschland AG in München. Er beschäftigt sich mit aktuellen Themen der offensiven IT-Sicherheit.