

Funktionsumfang

Alle 104 Funktionen in 14 Gruppen. Aufgeführt ist, was vorhanden ist: nichts davon ist angekündigt oder in Arbeit.

Erkennt Angreifer, ohne sie zu kennen

Keine Mustererkennung, die neuen Angriffen hinterherläuft. Der Hub misst, was ein Angreifer im Netz tun muss, und erkennt jeden, der sich umsieht, egal womit.

Alles in einer Software

Bestandsaufnahme, Fallen, Anmeldeüberwachung, Sensor, Eingriff im Haus und Beweissicherung unter einer Haube, mit einer Oberfläche. Die Netzdaten bleiben im Betrieb.

01 Bestandsaufnahme des Netzes

9

- **Geräteverzeichnis** mit Hersteller, Betriebssystem, offenen Diensten und Versionsständen
- **Herstellererkennung an der MAC-Adresse**, auch bei Geräten, die sonst nichts über sich verraten
- **Namen aus mehreren Quellen** — Router, Namensauflösung, Verzeichnisdienst: Ein Gerät, das nur als Adresse dasteht, wird von niemandem wiedererkannt
- **Veränderungserkennung**: neue Geräte, neu geöffnete Dienste, geänderte Versionsstände, verschwundene Geräte — jeweils gegenüber dem letzten Lauf
- **Karteileichen**: Geräte, die seit Tagen nicht mehr antworten, aber noch im Verzeichnis stehen
- **Geräte, die beim Scan geschlafen haben**, werden als solche geführt statt stillschweigend als „weg“ — ein abgeschalteter Rechner ist kein Befund
- **Rücksicht auf empfindliche Geräte**: Einbruchmeldeanlagen, Telefonanlagen, Labortechnik und Drucker lassen sich vom aktiven Scan ausnehmen
- **Prüfung von Switches, Routern und Access Points** über ihre Verwaltungsoberflächen — Geräte, die bei üblichen Scans durch das Raster fallen
- **Das zu prüfende Netz steht im Formular**, nicht in einer Datei hinter SSH — mit Vorschlag aus der vorhandenen Verkabelung und Prüfung der Eingabe

02 Härtungsprüfung der Systeme

6

- **Windows**: über zwanzig Prüfpunkte je System — Kennwortablage, SMB-Signierung, LSA-Schutz, Defender, Firewall, BitLocker, PowerShell-Protokollierung, automatische Anmeldung
- **Linux**: SSH-Konfiguration, Konten mit root-Rechten, ausstehende Sicherheitsaktualisierungen, Firewall, Protokollierung
- **Active Directory**: Kennwortrichtlinien, veraltete Konten, Dienstkonten, Anmeldeeinstellungen
- **Zertifikatdienste (ADCS)**: Vorlagen, die eine Rechteauserweiterung erlauben
- **Ohne Installation auf Ihren Rechnern**: Abgefragt wird über die Bordmittel, die Windows und Linux dafür mitbringen
- **Warum ein Rechner sich der Prüfung entzogen hat**, steht einzeln dabei: kein Zugang eingerichtet, Name nicht auflösbar, Anmeldung abgelehnt, Rechner aus. Nur der dritte Fall ist ein blinder Fleck — und genau der geht in einer Zahl wie „4 nicht erreichbar“ unter.

03 Was das Regelwerk bewertet

8

- **Klartext-Protokolle** — Telnet, FTP, POP3/IMAP ohne TLS, LDAP, VNC
- **Offene Datenbanken** — Redis, MongoDB, Elasticsearch, MySQL, PostgreSQL, MS SQL
- **Verwaltungszugänge** — IPMI/BMC, SNMP, RDP, NFS
- **TLS-Konfiguration** — veraltete Verfahren und schwache Cipher-Suites

- **SMB-Signierung nicht erzwungen** — der Weg, über den ein Angreifer im Windows-Netz fremde Anmeldungen weiterreicht
- **Werkseinstellungen auf Weboberflächen** — das Standardkennwort, das nie geändert wurde
- **Betriebssysteme ohne Updates** — Windows XP bis 8, Server 2003 bis 2012
- **Schwachstellensuche gegen bekannte Lücken** — auf Wunsch zusätzlich, je Treffer mit Fundstelle, gebündelt und nach der Wichtigkeit Ihrer Geräte gewichtet (setzt ein zusätzliches Prüfprogramm auf dem Hub voraus)

Jeder Befund nennt Beleg, Auswirkung und Maßnahme. **Es steht immer dabei, woran er erkannt wurde** — ein Befund, den niemand nachprüfen kann, ist eine Behauptung.

04 Außenseite und Router

7

- **Öffentliche Adresse** und ihre Chronik — wann sie gewechselt hat. Diese Auskunft lässt sich hinterher nicht rekonstruieren; ohne sie ist kein Vorfall einem Anschluss zuzuordnen
- **Offene Portfreigaben** am Router, vollständig und mit Ziel
- **Prüfung von außen:** welche Ports von der öffentlichen Seite tatsächlich antworten — nicht nur, was der Router zu erlauben meint
- **UPnP:** Kann sich ein Gerät im Netz selbst eine Tür ins Internet öffnen?
- **Ereignisprotokoll des Routers:** gescheiterte Anmeldungen an seiner Oberfläche, VPN-Verbindungen, Adresswechsel
- **Geräteauskunft:** unter welchem Namen ein Gerät im Router steht und **wie** es verbunden ist — LAN-Port, WLAN oder Gastzugang
- **Bekannt oder neu, mit Frist:** Ein Gerät, das der Router seit Wochen kennt, ist etwas anderes als eines, das seit zehn Minuten da ist. Ein Gerät im Gastzugang gilt nie als bekannt.

05 Fallen

9

- **Köderdateien** auf Ihren Dateiservern, zwischen echten Dateien statt in einem eigenen Ordner — wer sie anfasst, hat sie gesucht
- **Eigene Köderfreigaben auf dem Hub**, drei nebeneinander, jede mit eigenem Ordner und eigenem Konto. Sie stehen in keinem Anmeldeskript und in keiner Gruppenrichtlinie; wer sie ansteuert, hat sie gesucht.
- **Der Hub erscheint in der Windows-Netzwerkumgebung** — eine Falle, die niemand findet, ist keine
- **Köderkonten**, die nirgends hinterlegt sind und für nichts benutzt werden
- **Köderports:** Dienste, die es nicht gibt. Wer anklopft, sucht nach Angriffszielen.
- **Namensfalle:** Der Hub fragt nach Rechnernamen, die es nicht gibt. Wer darauf antwortet, fängt Anmeldedaten ab.
- **Erkennung am Verhalten:** Ein Angriffsprogramm durchsucht eine Freigabe in Sekunden, ein Mensch klickt sich langsam durch. Diesen Unterschied messen wir.
- **Was der Hub weiß, hängt davon ab, wo die Falle liegt.** Auf seiner eigenen Freigabe steht der Zugriff im Protokoll des Dateidienstes — mit Konto, Adresse und Arbeitsstation. Auf einem fremden Dateiserver sieht er, *dass* eine Köderdatei gelesen wurde, nicht von wem; wer zu dieser Zeit eine Sitzung offen hat, steht als Indiz daneben. Beides nebeneinander ist die stärkste Aufstellung.
- **Anmeldeversuch mit einem Köderkonto:** Schon ein gescheiterter Versuch zählt als Angriff. Die Köderkennwörter sind absichtlich falsch, wer es trotzdem probiert, hat das Konto gesucht.

06 Der Sensor auf Servern und Arbeitsplätzen

12

Option, nicht Pflicht — für Windows und für Linux. Er schließt die drei Lücken, die eine Prüfung von außen nicht sieht.

- **Fehlgeschlagene Anmeldungen und gesperrte Konten**, auch die, die nie am Domain Controller vorbeikommen
- **Neue lokale Konten, neue Dienste, neue geplante Aufgaben** — stündlich gegen den letzten Stand verglichen, damit ein Fund auch dann entsteht, wenn die Protokollierung dafür ausgeschaltet ist
- **Neue Verwalterrechte und Kerberoasting** — die Aufnahme in eine Verwaltergruppe, erkannt unabhängig von der Sprache des Systems, und das Sammeln von Anmeldetickets am Domain Controller

- **Welches Konto welche Freigabe verbunden hat** — auf Windows- wie auf Samba-Dateiservern, als Grundlage für die Nachverfolgung verdächtiger Konten
- **Ein geleertes Sicherheitsprotokoll** ist der schwerste Fund überhaupt: Es leert sich nicht von selbst, und im Alltag leert es niemand
- **Das Access-Log des Reverse Proxys**, wenn auf dem Rechner einer läuft (Traefik, nginx, Caddy): jede Zeile, alle zehn Sekunden — die einzige Stelle, an der ein Einbruch über einen Dienst im Internet sichtbar wird
- **Jede Minute ein Lebenszeichen**, auch wenn nichts geschehen ist. Gerade dann: Nur ein Strom, der im Normalfall fließt, kann versiegen.
- **Schweigen ist ein Fund** — aber erst nach der Gegenprobe: Antwortet der Rechner, während sein Sensor schweigt, hat jemand den Sensor abgeschaltet. Ist der Rechner aus, ist das Schweigen erklärt.
- **Die Abdeckung steht neben dem Bestand**: welche bekannten Geräte *keinen* Sensor haben. Der Eindruck vollständiger Abdeckung ist gefährlicher als eine sichtbare Lücke.
- **Jede Meldung ist einzeln signiert**. Der Hub kennt nur den öffentlichen Schlüssel — auch ein übernommener Hub kann keine Meldung fälschen.
- **Was er nie tut**: Befehle annehmen, sich selbst aktualisieren, vor Ort urteilen, als Administrator laufen, sich verstecken. Es gibt keinen Kanal, über den ihm jemand etwas aufträgt — auch wir nicht.
- **Was er einmal einstellt, steht in der Übergabe**: Bei Installation und Aktualisierung schaltet er die Aufzeichnung ein, die er braucht (unter Windows die Überwachungsrichtlinie, unter Linux die Samba-Protokollierung) — eng gefasst, mit Gegenprobe, abwählbar und beim Entfernen zurückgenommen. Im Betrieb liest er nur.

07 Anmeldungen im Windows-Netz

4

- **Angriffe auf die Anmeldeverfahren** — durchprobierte Kennwörter am Verzeichnisdienst, unterschieden nach geratenem Kennwort und geratenem Kontonamen: Das eine ist ein Tippfehler, das andere eine Suche
- **Anmeldeversuche an der eigenen Freigabe**, auch die gescheiterten: Konto, Arbeitsstation, Adresse, Ergebnis
- **Windows und Linux in einem Bild**: Ein durchprobirtes Kennwort wird erkannt, ob es an einem Windows-Server oder an einem Linux-Dienst scheitert
- **Der Hub schaltet die nötige Protokollierung selbst** ein, statt sie abzuschreiben — eng gefasst, mit Gegenprobe und rücknehmbar

08 Übernommene Konten

5

- **Eindeutige Spuren an einem Konto**: ein Kennwort, das von einer Stelle aus durchprobiert wird (nachts ab dem ersten Versuch, tagsüber ab dem dritten), mehrere Konten, die von derselben Stelle nacheinander probiert werden, eine Anforderung von Anmeldetickets in veralteter Verschlüsselung (Kerberoasting), die Aufnahme in eine Verwaltergruppe — Domänen-Admins ebenso wie sudo auf einem Linux-Server
- **Verdächtiges Konto an den echten Daten**: Geht ein Konto mit Spur binnen 24 Stunden auf eine Freigabe, wird gemeldet — in welcher Reihenfolge auch immer. Ein Zugriff allein ist Alltag, eine Spur allein steht im Protokoll.
- **Nachverfolgung**: zu jedem verdächtigen Konto jede Freigabe, auf der es in den letzten 30 Tagen war — und ausdrücklich, wenn es auf keiner war
- **Welche Ordner und Dateien**: je Konto jeder Ordner und jede Datei, die es geöffnet, geändert oder gelöscht hat, mit Zeitraum, Anzahl und Herkunft. Abgeholt bei den Dateiservern, sobald ein Verdacht besteht — Windows wie Linux (Samba). Daneben steht je Server, ob die Aufzeichnung lief und wie weit sie zurückreicht: Eine leere Liste ist sonst keine Auskunft.
- **Die nötige Aufzeichnung stellt der Sensor selbst her** — bei Installation und Aktualisierung, passend zur Rolle des Rechners, mit Gegenprobe. Ob sie hält, meldet er dem Hub mit jedem Lebenszeichen.

09 Überwachung im Netz

5

- **ARP-Überwachung**: Wenn ein Gerät die Adresse eines anderen übernimmt, um dessen Verkehr über sich zu lenken, steht es in der Tabelle
- **Gateway-Wache**: Ein Router, der plötzlich eine andere Kennung hat, ist der Fall, bei dem alles andere zu spät kommt

- **Spurensuche auf den Systemen:** neue Verbindungen nach draußen, neue Dienste, neue Autostart-Einträge, neue Konten — gemeldet wird die Veränderung, nicht ein Name von einer Liste
- **Verbindungsjournal am Spiegelport,** wo einer eingerichtet ist: je Verbindung eine Zeile — wer sprach wann mit wem, wie lange und wie viel. **Kein Mitschnitt,** kein Inhalt, kein aufgehobenes Paket.
- **Ortung am Switch:** zu jedem Gerät der Port, an dem es hängt — damit ein Fund eine Buchse hat und nicht nur eine Adresse

10 Bewertung und Meldung

6

- **Alarmmatrix:** Für jedes Erkennungsverfahren steht einzeln ein, ab welcher Einstufung gemeldet und ab welcher eingegriffen wird
- **Gewichtung mit nachvollziehbaren Gründen:** außerhalb der Geschäftszeiten, Gerät nicht im Verzeichnis, zufällige MAC-Adresse, mehrere Funde desselben Geräts, Zugriff aus dem Internet — jeder Grund steht in der Zeile
- **Angriffsprotokoll** über alle Verfahren hinweg, in einer Tabelle: Die Einzelprotokolle werden dafür gelesen und zusammengeführt, nicht ersetzt — jede Zeile behält ihre Herkunft und ihre Einzelheiten
- **Eigene Prüfläufe melden sich vorher an** und lösen deshalb keinen Alarm aus — ohne dass dafür eine Adresse pauschal ausgenommen würde
- **Alarmierung** per E-Mail, Webhook oder Push-Nachricht, mit täglicher Bestätigung, dass die Überwachung läuft. Bleibt sie aus, wissen Sie es.
- **Prüfbetrieb:** befristet und mit Grund angekündigt — die Funde stehen im Protokoll, die Maßnahmen ruhen

11 Was im Angriffsfall automatisch geschieht

6

- **Sitzung kappen:** Die Verbindung des Angreifers zur Freigabe wird beendet
- **Switch-Port abschalten:** Das Gerät ist vom Netz. Der Port geht nach einer einstellbaren Frist von selbst wieder an, oder sofort auf Knopfdruck.
- **Internetverbindung kappen:** der grobe Hebel, ab Werk abgeschaltet — er nimmt allen den Weg nach draußen und dazu den Alarmweg
- **Nachts strenger als tags:** Bei manchen Verfahren entscheidet die Tageszeit, ab wann eingegriffen wird — um drei Uhr früh sucht niemand versehentlich
- **Jeder Eingriff hat einen Rückweg,** und er steht in der Oberfläche
- **Kein Eingriff gegen den Hub selbst:** Er nähme die Falle mit vom Netz

12 Beweissicherung

10

- **Vorfallsakte bei jedem Fund,** angelegt vor dem Eingriff: offene Sitzungen, vollständige ARP-Tabelle, wer am verdächtigen Gerät angemeldet ist
- **Verbindungen des verdächtigen Geräts nach draußen** — damit wird sichtbar, von welcher öffentlichen Adresse aus ein gekappter Rechner ferngesteuert wird. Bis dahin endete die Spur bei der internen Adresse.
- **Zwei Adressen auf einer MAC** werden ausgerechnet und hervorgehoben: das Bild einer Umleitung, und der Augenblick des Fundes ist der einzige, in dem es dasteht
- **Die verdächtigen Konten stehen in jeder Sicherung** — mit ihren Spuren, ihren Freigaben und jedem Ordner und jeder Datei, die sie angefasst haben. Die Frage nach einem Vorfall ist fast immer dieselbe: *Was hat er gesehen?*
- **Zeitanker:** die Uhr des Hubs, damit sich die Akte neben fremde Protokolle legen lässt
- **Prüfsummen und eine Kette:** Jede Sicherung trägt Prüfsummen über ihre Dateien und ist mit der vorherigen verkettet. Wer den jüngsten Kettenwert einmal außer Haus schafft — ausgedruckt, per Mail, beim Steuerberater —, kann später belegen, dass keine Sicherung verändert und keine entfernt wurde.
- **Auch das Scheitern steht in der Akte.** Eine Lücke, die aussieht wie „nichts gefunden“, wäre das Gegenteil eines Nachweises.
- **Zwei Berichte aus einer Sicherung** — einer für die Geschäftsleitung (was ist passiert, wie schlimm ist es, was ist zu entscheiden, was wissen wir nicht), einer für die IT mit den technischen Einzelheiten. Ein Bericht, der beide Fragen beantwortet, beantwortet keine.

- **Protokolle werden nicht gelöscht, sondern beiseitegelegt** — mit Zeitstempel, auffindbar. Nach einem Fehlalarm sind sie der Beleg, dass es einer war.
- **Herkunft eines Angreifers aus dem Internet:** Netzbetreiber, Land und Abuse-Kontakt aus der Adressvergabestelle, als eigene Zeile in Sicherung und Bericht. Adressen aus dem eigenen Netz werden nie nachgefragt.

13 Der Hub schützt sich selbst

6

Wer eine Erkennung ausschaltet, tut das nicht spurlos — für einen Angreifer, der es bis auf den Hub geschafft hat, wäre genau das der erste Griff.

- **Einstellungsprotokoll:** wer wann von wo aus was verstellt hat. Es lässt sich nicht leeren.
- **Gemeldet wird, was die Erkennung schwächt** — eine ausgeschaltete Wache, eine geleerte Alarmmatrix, eine entfernte Falle
- **Die Wachen überstehen einen Neustart.** Was laufen soll, steht auf der Platte und nicht im Arbeitsspeicher: Nach Stromausfall oder Aktualisierung läuft es wieder an, ohne dass jemand daran denkt.
- **Bereitschaftsprüfung:** Der Hub sagt vorher, was er kann und was ihm fehlt. Jede Voraussetzung, die fehlt, meldet sich **vorher** — nicht im Ernstfall durch Stillstand.
- **Überfällige Prüfläufe stehen rot**, statt still auszufallen
- **Selbsttest der Erkennung:** Der Hub spielt den Angreifer und weist nach, dass die Falle wirklich anschlägt

14 Betrieb und Bedienung

11

- **Weboberfläche** im Browser, ohne Installation auf Ihren Arbeitsplätzen — mit Anmeldung, auch hinter einem vorhandenen Reverse Proxy zu betreiben
- **Zeitplan:** Prüfläufe laufen von selbst, zu den Zeiten, die Sie festlegen. Ein Lauf, der wegen eines Neustarts ausfiel, wird nachgeholt statt übersprungen.
- **Berichte** als lesbares Dokument und als PDF, nicht als Rohdatenausgabe
- **Aufräumen mit Unterschied:** Ergebnisdateien werden gelöscht, Protokolle nur mit Zeitstempel beiseitegelegt, und die Vergleichsstände bleiben stehen — ohne sie wäre jeder folgende Lauf wieder ein Erstlauf und seine Ruhe erfunden
- **Einstellungen in Reitern** — Netz, Zugang, Köder, Switch, Alarmierung, Betrieb — statt einer langen Seite; offene Punkte der Bereitschaft stehen als Zahl am Reiter
- **Deutsch und Englisch** in derselben Oberfläche umschaltbar
- **Anleitungen und Kundendokumente liegen auf dem Gerät** und reisen mit jedem Stand mit
- **Läuft auf einem Kleinrechner** im Netz — kein Serverschrank, kein Cloud-Konto
- **Ohne Internet arbeitsfähig:** Die Lizenz wird einmal aktiviert und nur gelegentlich erneuert. Fällt der Lizenzserver aus oder fehlt das Internet, arbeitet der Hub weiter; rechtzeitig vor Ablauf warnt er, und die Erneuerung geht auch per Datei
- **Jede Auslieferung trägt eine Nummer**, und zu jeder Nummer steht nachlesbar, was sich geändert hat
- **HTTPS auf Knopfdruck:** Der Hub erzeugt sein Zertifikat selbst und startet verschlüsselt neu, auch ohne vorgeschalteten Reverse Proxy