

Wogegen wir schützen — und wie

Alle Funktionen in einfachen Worten. Für jede steht hier, welchen Angriff sie erschwert oder sichtbar macht — und was sie dafür tut.

Fassung Oktober 2026 Für Geschäftsführung, IT-Verantwortliche Lesedauer etwa 15 Minuten

Wie ein Angriff wirklich abläuft

Fünf Schritte — und an jedem steht etwas im Weg

Ein Einbruch ins Firmennetz ist selten ein einzelner Moment. Er ist eine Kette. Jedes Glied davon braucht Zeit, und jedes hinterlässt Spuren. Wer nur das letzte Glied absichert — die Daten —, merkt erst etwas, wenn sie weg sind. Wir setzen deshalb an jedem Glied an.

1 Hineinkommen

Eine E-Mail mit Anhang. Ein Gerät, das niemand mehr kennt und das seit Jahren dasselbe Werkskennwort hat. Ein Fernzugang, der für einen Techniker geöffnet und nie geschlossen wurde. Fast immer ist es einer dieser drei Wege — spektakuläre Methoden sind die Ausnahme.

Unsere Antwort: Wir zeigen Ihnen, welche Geräte es überhaupt gibt, welche Dienste davon aus dem Netz erreichbar sind, welche noch mit Werkseinstellungen laufen — und welche Türen Ihr Router nach außen offen hält.

2 Sich umsehen

Wer drin ist, weiß zunächst nichts. Kein Angreifer kennt Ihr Netz. Er muss suchen: Welche Rechner gibt es? Wo liegen Dateien? Wer ist Administrator? Dieser Schritt kommt **immer**, und er ist laut — vorausgesetzt, jemand hört hin.

Unsere Antwort: Wir stellen ihm Dinge in den Weg, die es gar nicht gibt. Dateien, die niemand öffnen dürfte. Dienste, die niemand ansprechen dürfte. Rechnernamen, nach denen niemand fragen dürfte. Wer darauf zugreift, hat gesucht — und sich damit verraten.

3

Sich ausbreiten

Ein einzelner Rechner nützt wenig. Der Angreifer will die Zugangsdaten eines Administrators, denn damit gehört ihm alles. In Windows-Netzen gibt es dafür seit Jahren dieselben, gut bekannten Wege — sie funktionieren nur, wenn bestimmte Einstellungen nicht gesetzt sind.

Unsere Antwort: Wir prüfen genau diese Einstellungen, auf jedem Rechner und in der Benutzerverwaltung. Und wir legen Zugangsdaten aus, die echt aussehen, aber zu Konten gehören, die nur eines können: melden, dass jemand sie ausprobiert hat.

4

Zugreifen

Jetzt erst passiert der Schaden: Daten werden kopiert, verschlüsselt oder beides. Ein Verschlüsselungstrojaner arbeitet dabei stur eine Freigabe nach der anderen ab — er kann nicht unterscheiden, welche Datei wichtig ist.

Unsere Antwort: Genau diese Blindheit nutzen wir. Zwischen Ihren echten Dateien liegen unsere. Sie werden angefasst wie alle anderen — nur schlägt bei ihnen der Alarm an, während der Rest noch unberührt ist.

5

Wiederkommen

Wer einmal drin war, will zurück. Also richtet er sich ein: ein Programm, das bei jedem Start mitläuft. Ein zusätzliches Benutzerkonto. Eine Verbindung nach draußen, die offen bleibt. Eine Freigabe im Router, die er sich selbst öffnet.

Unsere Antwort: Wir merken uns, wie Ihre Rechner aussehen, wenn alles in Ordnung ist — und melden, was seither dazugekommen ist. Nicht alles Neue ist ein Angriff, aber jeder Angriff ist etwas Neues.

Was überhaupt da ist

Die Grundlage — man kann nicht schützen, was man nicht kennt

Die meisten Betriebe wissen nicht genau, was in ihrem Netzwerk hängt. Das ist kein Vorwurf: Über Jahre kommen Drucker, Kameras, Steuerungen, Telefonanlagen und Testrechner dazu, und niemand führt Buch. Genau diese Lücke ist der bequemste Einstieg.

Geräteverzeichnis

Schützt gegen: das vergessene Gerät, das niemand mehr pflegt — und das deshalb noch offen steht.

Wir fragen jedes Gerät im Netz: Wer bist du? Was läuft auf dir? Heraus kommt eine Liste mit Hersteller, Betriebssystem und allen Diensten, die von außen ansprechbar sind. Bei stillen Geräten, die kaum antworten, hilft die Geräteerkennung der Netzwerkkarte weiter — sie verrät zumindest den Hersteller und ob mehrere Adressen zum selben Gerät gehören.

FÜR DIE TECHNIK

nmap als Erhebungsbasis, drei Scan-Tiefen. Auswertung der NSE-Skriptausgaben im Profil [thorough](#). Geräteidentifikation über die OUI-Datenbank der MAC-Adressen; mehrere IPs auf einer MAC werden als dasselbe Gerät erkannt.

Bewertung der offenen Dienste

Schützt gegen: Dienste, die im Netz erreichbar sind, ohne dass es jemandem noch bewusst wäre.

Eine Liste offener Ports hilft niemandem. Wir sagen stattdessen im Klartext, was daran ein Problem ist, was im schlimmsten Fall passiert und was zu tun ist. Erkannt werden unter anderem: Verbindungen, bei denen Kennwörter unverschlüsselt über die Leitung gehen; Datenbanken ohne Zugangsschutz; Fernwartungs- und Verwaltungszugänge; veraltete Verschlüsselung; Geräte mit Werkskennwörtern; Betriebssysteme, für die es seit Jahren keine Sicherheitsupdates mehr gibt.

Jeder Befund bekommt eine Einstufung. Steht das betroffene Gerät auf Ihrer Liste der wichtigen Systeme, steigt sie automatisch um eine Stufe — derselbe Fehler wiegt auf dem Warenwirtschaftsserver schwerer als auf einem Testrechner.

Veränderungserkennung

Schützt gegen: das Gerät, das gestern noch nicht da war — und den Dienst, den gestern noch niemand geöffnet hatte.

Jeder Lauf wird mit dem vorherigen verglichen. Gemeldet wird, was neu ist: ein Gerät, ein offener Zugang, eine geänderte Softwareversion. Das ist die einfachste und zugleich verlässlichste Art, Ungewöhnliches zu finden — sie braucht kein Wissen darüber, wie ein Angriff aussieht.

Netzwerkgeräte: Switch, Router, Access Point

Schützt gegen: die Übernahme der Geräte, über die der gesamte Verkehr läuft.

Diese Geräte tragen das ganze Netz und fallen bei üblichen Prüfungen durch jedes Raster — sie antworten auf die Standardfragen schlicht nicht. Wir prüfen sie deshalb gesondert, vor allem ihre Verwaltungsoberfläche: Geht das Kennwort dorthin unverschlüsselt über die Leitung? Wer den Verkehr mitliest, hat damit die Kontrolle über das Netz, in dem alle anderen Systeme stehen.

Wer sich der Prüfung entzogen hat

Schützt gegen: die trügerische Ruhe eines Berichts, in dem die interessanten Geräte einfach fehlen.

„Vier Geräte nicht erreichbar“ ist keine Auskunft, sondern deren Verweigerung. Dahinter können vier verschiedene Sachverhalte stehen, und jeder verlangt eine andere Antwort. Wir schlüsseln das auf, statt es stillschweigend zu übergehen. Ein Rechner, der schweigt, gilt bei uns nicht als ruhig, sondern als stumm.

Die Systeme selbst

Nicht was von außen erreichbar ist, sondern wie es eingestellt ist

Ein Netzwerk-Scan sieht nur die Oberfläche. Die entscheidenden Einstellungen liegen darunter — und es sind fast immer dieselben, die einen Angreifer vom einzelnen Rechner zur Kontrolle über den ganzen Betrieb bringen.

Windows-Rechner und -Server

Schützt gegen: den Diebstahl von Zugangsdaten im eigenen Netz — den häufigsten Weg zur Ausbreitung.

Über zwanzig Prüfpunkte je System. Der wichtigste Block betrifft eine Eigenart von Windows: Rechner rufen im Netz nach Namen, die sie nicht finden, und glauben dem Ersten, der antwortet. Ein Angreifer antwortet einfach immer — und bekommt so Anmeldedaten frei Haus. Wir prüfen, ob die Einstellungen gesetzt sind, die genau das verhindern.

Dazu kommen: ob Kennwörter im Arbeitsspeicher im Klartext liegen, ob die Festplatte verschlüsselt ist, ob der Virenschutz tatsächlich läuft und aktuell ist, ob die Firewall vollständig aktiv ist, ob sich jemand automatisch mit gespeichertem Kennwort anmeldet, ob eine Freigabe für „Jeden“ offen steht und wann zuletzt Sicherheitsupdates eingespielt wurden.

Ein Befund verdient dabei besondere Erwähnung: Wenn mehrere dieser Einstellungen zusammen fehlen, ergibt das keinen Einzelfehler mehr, sondern einen durchgehenden Angriffsweg. Diesen Zusammenhang benennen wir ausdrücklich, statt drei harmlos wirkende Hinweise nebeneinander zu stellen.

FÜR DIE TECHNIK

LLMNR, mDNS, NetBIOS, SMB-Signierung ein- und ausgehend, SMBv1, LDAP-Signierung, WDigest, LSA-Schutz, AutoLogon, Firewallprofile, BitLocker, Defender-Echtzeitschutz und Signaturalter, UAC, PowerShell-Protokollierung und -Version 2.0, Sysmon, RDP mit NLA, Freigaben mit „Jeder“, Alter des letzten Sicherheitsupdates. Zusätzlich die zusammengesetzte Kette [Hash abfangen und weiterreichen](#).

Linux-Systeme

Schützt gegen: Server, die still im Keller laufen und seit Jahren niemand angesehen hat.

Geprüft wird der Fernzugang (ist Anmeldung mit Kennwort statt Schlüssel möglich? Darf sich der Hauptbenutzer direkt anmelden?), ob es weitere Konten mit vollen Rechten gibt, ob ein Konto ganz ohne Kennwort existiert, ob Sicherheitsaktualisierungen ausstehen oder gar nicht mehr kommen, ob eine Firewall läuft, ob die Protokollierung einen Neustart übersteht und ob Systemdateien für jeden beschreibbar sind.

Benutzerverwaltung (Active Directory)

Schützt gegen: den Sprung vom normalen Mitarbeiterkonto zu Administratorrechten über das ganze Haus.

Die zentrale Benutzerverwaltung ist der Generalschlüssel. Wir prüfen die Kennwortregeln, ob Konten nach Fehlversuchen gesperrt werden, wie viele Administratoren es tatsächlich gibt, ob Dienstkonten mit alten Kennwörtern herumstehen, ob einzelne Konten sich für andere ausgeben dürfen und ob die Kennwörter der lokalen Administratoren zentral verwaltet werden statt überall gleich zu lauten.

Das ist kein akademischer Punkt: Mehrere dieser Einstellungen erlauben es, mit ganz gewöhnlichen Benutzerrechten an Administratorkennwörter zu kommen — ohne Sicherheitslücke, allein durch die Konfiguration.

FÜR DIE TECHNIK

Kontosperrung, Passwortlänge und -komplexität, umkehrbare Verschlüsselung, abschwächende Fine-Grained Policies, MachineAccountQuota, krbtgt-Alter, LAPS-Abdeckung, unbeschränkte und beschränkte Delegation inklusive RBCD, Kerberoasting-Angriffsfläche (SPN-Konten), AS-REP-Roasting, DES und RC4, Besetzung der privilegierten Gruppen.

Zertifikatdienste

Schützt gegen: einen der kürzesten bekannten Wege vom Benutzerkonto zur vollständigen Übernahme.

Wenn Ihr Haus eigene digitale Ausweise ausstellt, kommt es auf die Regeln an, nach denen das geschieht. Sind sie zu großzügig, kann sich ein gewöhnlicher Benutzer einen Ausweis ausstellen lassen, der auf den Namen des Administrators lautet — und sich damit anmelden. Ohne dessen Kennwort, ohne Alarm. Wir prüfen die Vorlagen und die Rechte auf der Ausstellungsstelle.

Merken, dass jemand da ist

Der Teil, den ein Virens Scanner nicht leistet

Alles bisher Genannte verringert die Angriffsfläche. Dieser Abschnitt setzt voraus, dass es trotzdem passiert ist. Die Idee dahinter ist einfach: Ein Angreifer muss suchen. Also legen wir ihm Dinge in den Weg, die es nur für ihn gibt — **jeder Zugriff darauf ist ein Treffer**, kein Verdacht, keine Auslegung.

Der Ruf nach Rechnern, die es nicht gibt

Schützt gegen: das Mitschneiden von Anmeldungen im eigenen Netz — den gängigsten Einstieg in ein Windows-Netz.

Wir rufen ins Netz hinein: „Wo ist der Rechner SRV47?“ Den gibt es nicht; wir haben ihn erfunden, passend zu den Namen, die bei Ihnen wirklich vorkommen. Ein normales Gerät kennt ihn nicht und schweigt. Ein Angreifer mit dem üblichen Werkzeug *muss* antworten — „Der bin ich!“ —, denn genau davon lebt er.

Gefragt wird immer nach zwei erfundenen Namen. Ein echtes Gerät könnte zufällig wie einer davon heißen; auf beide antwortet nur, wer auf alles antwortet. Und wir schicken niemals eine Anmeldung hinterher — sonst ginge genau das Kennwort über die Leitung, um dessen Schutz es geht.

Die erfundenen Namen entstehen jedes Mal neu aus Ihrem Netz. Ein fester Name stünde im Programm und wäre auslesbar — ein Angreifer würde seinem Werkzeug beibringen, ausgerechnet darauf nicht zu antworten, und die Erkennung meldete ab da still „alles in Ordnung“.

FÜR DIE TECHNIK

LLMNR-, NBT-NS- und mDNS-Anfragen aus dem eigenen Segment. Kein Mirror-Port nötig: Broadcast und Multicast kommen an jedem Port an. Aktiv gefragt statt gelauscht, weil die Antworten per Unicast zurückgehen und für einen Mithörer unsichtbar wären.

Dateien, die niemand öffnen dürfte

Schützt gegen: Datendiebstahl und Verschlüsselungstrojaner — und zwar bevor der Schaden vollständig ist.

Auf Ihren Freigaben liegen Dateien mit Namen, nach denen gesucht wird: Bankkonten, Zugangsdaten, Gehaltsliste. Sie liegen **zwischen Ihren echten Dateien**, nicht in einem eigenen Ordner — ein Ordner, in dem verdächtig ordentlich nur Interessantes liegt, fällt auf. Ihre Mitarbeiter haben keinen Anlass, sie zu öffnen. Wer es doch tut, hat gesucht.

Es sind echte, funktionierende Tabellen mit plausiblen Inhalt und gealterten Zeitstempeln. Eine Datei, die sich nicht öffnen lässt, macht einen aufmerksamen Angreifer misstrauisch, bevor die Falle zuschnappt.

Zugangsdaten, die nicht funktionieren

Schützt gegen: die Verwertung gestohlener Zugangsdaten — der Schritt zwischen Fund und Schaden.

In diesen Dateien stehen Benutzernamen und Kennwörter. Die Konten gibt es wirklich, das Kennwort ist falsch. Wer es ausprobiert, scheitert — und hinterlässt dabei genau den Anmeldeversuch, auf den es ankommt. Das ist der Unterschied zwischen „jemand hat die Datei gesehen“ und „jemand verwertet sie gerade“.

Wer an den Konten rüttelt

Schützt gegen: das Erraten von Kennwörtern, das Durchprobieren vieler Konten und das heimliche Verschaffen von Verwalterrechten.

Jeder Server schreibt mit, wenn eine Anmeldung scheitert. Der Hub liest das — beim Domain Controller und über den Sensor auf Servern und Linux-Rechnern — und unterscheidet: Ein Name, den es nicht gibt, ist Raten; ein falsches Kennwort zu einem echten Konto heißt, jemand kennt den Namen. Mehrere Konten von derselben Stelle in einer Stunde sind ein Angriff, der unter jeder Sperrschwelle bleiben will. Dazu fallen auf: ein Konto, das Dienst-Tickets zum Knacken sammelt, ein Konto, das plötzlich Verwalterrechte bekommt, und ein neues Konto auf einem Server.

Verdächtige Konten an den echten Daten

Schützt gegen: den Datendiebstahl mit einem übernommenen Konto — auf den echten Freigaben statt in der Falle.

Auf die Freigaben gehen jeden Morgen alle; jeden Zugriff zu melden hilft nicht. Der Hub merkt sich deshalb, welches Konto wann welche Freigabe geöffnet hat, und meldet, sobald ein Konto mit einer eindeutigen Spur — siehe oben — innerhalb eines Tages an die Daten geht. Zu jedem verdächtigen Konto steht in der Oberfläche, wo es in den letzten 30 Tagen war. Windows- wie Linux-Dateiserver.

Dienste, die es nicht gibt

Schützt gegen: die Erkundung des Netzes und die Ausbreitung von Verschlüsselungstrojanern.

Wir halten ein paar einladende Zugänge offen, hinter denen nichts steht. Sie stehen in keiner Dokumentation, kein Gerät braucht sie, kein Programm hat je einen Grund, sie anzusprechen. Wer dort anklopft, sucht nach Angriffszielen — und Suchen ist der erste Schritt nach jedem Einbruch. Auch jeder Verschlüsselungstrojaner, der sich ausbreiten will, stolpert hier, bevor er etwas gefunden hat.

Beantwortet wird nichts. Die Verbindung wird angenommen, der Absender festgehalten, sofort geschlossen. Ein Köder, der etwas vortäuscht, wäre ein Dienst — und ein Dienst kann eine Schwachstelle haben.

Fremde Geräte im Netz

Schützt gegen: das eingeschmuggelte Gerät und die Umleitung des Datenverkehrs.

Wir vergleichen laufend, welche Geräteerkennung zu welcher Adresse gehört. Auffällig ist: eine bekannte Adresse, die plötzlich zu einem anderen Gerät gehört; ein Gerät, das gleich mehrere Adressen für sich beansprucht; ein Gerät, das in keinem Bestand steht.

Der Selbsttest

Schützt gegen: den teuersten aller Zustände — eine Überwachung, die blind ist, ohne dass es jemand merkt.

Eine leere Ereignisliste bedeutet zweierlei: „niemand war da“ oder „wir hätten es nicht gemerkt“. Das eine ist beruhigend, das andere gefährlich, und sie sehen gleich aus. Deshalb lässt sich jede Falle auf Knopfdruck auslösen. Erst wenn der Alarm dabei tatsächlich ankommt, ist die Ruhe im Bericht etwas wert.

Spuren auf den Rechnern

Sitzt bereits jemand auf einem unserer Systeme?

Den Einbruch selbst sieht man nicht — kommt er per E-Mail, findet er im Netz gar nicht statt. Was ein Eindringling hinterlässt, sobald er da ist, ist dagegen immer dasselbe, egal wie er hereinkam.

Was seit gestern dazugekommen ist

Schützt gegen: den Eindringling, der sich eingerichtet hat und auf seine Gelegenheit wartet.

Wir merken uns je Rechner, wie er im Normalzustand aussieht: welche Programme beim Start mitlaufen, welche Verbindungen nach draußen bestehen, welche Benutzerkonten es gibt, welche geplanten Aufgaben eingerichtet sind. Beim nächsten Lauf zählt nur der Unterschied.

Einzelnen ist nichts davon auffällig — deshalb funktioniert der Vergleich so gut. Eine Verbindung zu einer fremden Adresse ist alltäglich; eine Verbindung zu einer fremden Adresse, die gestern noch nicht da war und von einem Programm im temporären Ordner ausgeht, ist es nicht.

Die Tür nach außen

Was Ihr Router ins Internet offen hält

Portfreigaben und selbst geöffnete Rückwege

Schützt gegen: den Zugang von außen, für den niemand einen Benutzer anklicken muss.

Wir fragen den Router, welche Türen er nach außen offen hält, und vergleichen mit dem letzten Blick. Eine neue Freigabe ist ein Befund hoher Stufe: Hat sie niemand von Hand angelegt, hat ein Gerät im Netz sie sich selbst geöffnet. Das dürfen die meisten Router jedem Programm erlauben — ohne Kennwort, ohne Rückfrage, ohne dass es jemand bemerkt. Genau so baut sich Schadsoftware ihren Rückweg.

Der eigentliche Befund ist dabei nicht die Zahl der Freigaben, sondern die Frage, wer sie anlegen darf. Dass gerade keine besteht, ist eine Momentaufnahme und keine Eigenschaft Ihres Netzes.

Eine neue Freigabe erfahren Sie per E-Mail und Push, spätestens nach einer Viertelstunde — nicht erst, wenn jemand die Seite öffnet.

FÜR DIE TECHNIK

Zwei Wege: [UPnP](#) beantwortet unangemeldet die Frage, ob sich Geräte selbst freigeben können. [TR-064](#) liefert nach Anmeldung die vollständige Freigabetabelle – auch die von Hand eingetragenen Einträge, die über UPnP grundsätzlich unsichtbar bleiben. Empfehlung: UPnP abschalten, TR-064 mit eigenem Benutzer einschalten.

Wer sich im Router einrichtet

Schützt gegen: einen gekaperten Router, über den jemand dauerhaft hereinkommt oder Ihren Verkehr umleitet.

Wer einen Router übernimmt, muss dort etwas verstellen, damit es ihm nützt: den Fernzugang einschalten, einen Benutzer anlegen, einen anderen DNS-Server verteilen, eine Rufumleitung auf eine teure Nummer setzen. Wir merken uns die wichtigen Einstellungen Ihrer FRITZ!Box und vergleichen sie alle 15 Minuten. Ändert sich etwas, erfahren Sie es per E-Mail und Push, mit dem alten und dem neuen Wert.

Der Router sagt von sich aus nicht Bescheid, deshalb fragen wir regelmäßig nach. Für die sofortige Meldung schalten wir zusätzlich die Änderungsnotiz Ihrer FRITZ!Box ein. Die sitzt allerdings im Gerät, das angegriffen wird, und wer die Box übernimmt, schaltet sie als Erstes ab. Unsere Prüfung von außen kann er nicht abschalten — beides zusammen meldet sofort im Normalfall und spätestens nach einer Viertelstunde, wenn jemand die Notiz zum Schweigen gebracht hat.

Auch Ihre eigenen Änderungen melden sich. Das ist Absicht: Wer an der Box saß, können wir nicht wissen — und eine Meldung über die eigene Wartung kostet einen Blick, eine verschluckte fremde Änderung kostet den Anschluss.

FÜR DIE TECHNIK

Gezielte TR-064-Einzelabfragen, nur lesend: Benutzerliste, Fernzugang, DynDNS, MyFRITZ!, UPnP, DHCP und DNS, Zeitserver, jedes WLAN, Rufumleitungen, IP-Telefone, Rufnummern, Modell, Seriennummer und Firmware. Kennwörter nur als gesalzener Abdruck. Nicht abgedeckt: VPN, Rechte einzelner Benutzer, IPv6-Firewall, eine veränderte Firmware mit alter Versionsnummer und Software auf Geräten hinter dem Router.

Ihre öffentliche Adresse — lückenlos mitgeschrieben

Schützt gegen: den Fall, dass ein Vorfall aufgeklärt werden soll und die entscheidende Angabe fehlt.

Jeder Anschluss hat nach außen eine Adresse, und er behält sie nicht ewig — meist wechselt sie über Nacht. Wenn Wochen später auffällt, dass etwas passiert ist, und Sie beim Anbieter eine Auskunft brauchen, muss belegbar sein, welche Adresse Sie *zum Zeitpunkt des Vorfalls* hatten. Diese Angabe lässt sich hinterher nicht rekonstruieren.

Wir schreiben sie deshalb fortlaufend mit und sagen bei jeder Auskunft dazu, wie belastbar sie ist: Liegt der gefragte Zeitpunkt in einem Zeitraum, den wir tatsächlich beobachtet haben, gilt die Angabe. Liegt er in einer Lücke zwischen zwei Prüfungen, sagen wir das ausdrücklich. Eine Angabe, die nur wahrscheinlich stimmt, als sicher auszugeben, wäre hier der teuerste Fehler von allen.

Wer vor der Tür steht — die Dienste im Internet

Schützt gegen: den Einbruch über den Dienst, der absichtlich von außen erreichbar ist — und gegen die Frage hinterher, wie er hereingekommen ist.

Wer eine Videokonferenz, einen Chat oder einen Kennwortspeicher im Internet betreibt, hat eine Tür, die offen sein muss. Davor steht ein Türsteher — der Reverse Proxy —, und der schreibt jede Anfrage auf: wer, wann, welcher Dienst, welche Antwort. Diese Liste liest der Sensor auf dem Rechner des Türstehers mit und meldet jede Zeile. Die Oberfläche zeigt sie live und färbt rot, was nach Einbrecher aussieht: Anfragen nach Dateien, die es auf keinem ordentlichen Server zu holen gibt, abgewiesene Anmeldungen, Verwaltungsseiten von außerhalb, ein Dienst, hinter dessen Proxy nichts antwortet.

Das meiste davon ist Alltag — jede Adresse im Internet wird täglich von Automaten abgeklopft, und das melden wir nicht, sonst liest bald niemand mehr. Gemeldet wird, was darüber hinausgeht: mehrere abgewiesene Anmeldungen am Kennwortspeicher, eine Verwaltungsseite, die von draußen aufgeht, eine Datei, die tatsächlich ausgeliefert wurde. Und wenn doch einmal jemand hereinkommt, steht hinterher in dieser Liste, wie.

FÜR DIE TECHNIK

Access-Log von Traefik, nginx oder Caddy, gelesen vom Linux-Agenten auf dem Proxy-System ([Webprotokoll](#)), JSON oder CLF, alle 10 Sekunden. Eigene Ablage mit Aufbewahrungsfrist. Fünf Verfahren in der Alarmmatrix, keines mit Maßnahme: Gegen eine Adresse aus dem Internet gibt es im Haus nichts zu schalten. Was gegen die Scanner hilft, ist eine Middleware am Proxy, die Punktpfade mit 403 beantwortet — Anleitung im Technikerblatt.

Wenn es ernst wird

Von der Meldung zur Handlung

Alarm, der ankommt

Schützt gegen: die Meldung, die tagelang unbemerkt in einer Oberfläche steht.

Jeder Treffer geht sofort hinaus — per E-Mail oder an ein System Ihrer Wahl. Wiederholtes Anklopfen desselben Absenders wird zusammengefasst, damit aus einem Vorfall nicht zwanzig Meldungen werden.

Wo steckt das Gerät?

Schützt gegen: die Ratlosigkeit nach der Meldung — Kabel verfolgen, Geräte durchzählen, raten.

Jede Meldung endet zunächst bei einer Adresse. „192.168.178.47 ist neu im Netz“ beantwortet nicht die Frage, die als Nächstes kommt: *Wo steht das Ding?* Ihr Switch weiß es längst — er führt eine Tabelle, in der zu jedem Gerät der Anschluss steht, an dem es zuletzt gesprochen hat. Wir lesen sie aus und schreiben die Dose in der Wand direkt an die Meldung.

Dabei sagen wir auch, wie sicher die Zuordnung ist. Hängen an einem Anschluss mehrere Geräte, weil dort ein weiterer Switch sitzt, ist „Port 1“ eine Richtungsangabe und keine Ortung — und wird auch so ausgewiesen.

FÜR DIE TECHNIK

SNMPv2c, ausschließlich lesend; kein SNMP-SET im ganzen Modul. Q-Bridge- und Bridge-MIB, VLAN-fähig. Voraussetzung ist ein verwalteter Switch mit eingeschaltetem SNMP.

Was eine Anzeige braucht

Schützt gegen: den Verlust der Beweislage zwischen Vorfall und Aufklärung.

Jeder Fund wird als eigene Zeile festgehalten, mit den vier Angaben, die eine Auskunft beim Anbieter tatsächlich braucht: wann genau (mit Zeitzone), welche Gegenstelle, welcher Rechner, und welche öffentliche Adresse Sie zu diesem Zeitpunkt hatten.

Eine Voraussetzung können wir dabei nicht herstellen und sagen sie deshalb deutlich: **Die Uhr der Systeme muss stimmen.** Ein Zeitstempel, der drei Minuten falsch geht, macht die Auskunft wertlos.

Berichte, die jemand lesen kann

Schützt gegen: den Prüfbericht, den niemand durcharbeitet, weil er aus Rohdaten besteht.

Jeder Lauf erzeugt einen Bericht: Zusammenfassung, Befunde nach Dringlichkeit, je Befund der Beleg, die Auswirkung und die konkrete Maßnahme. Dazu ein Abschnitt, den kaum ein Werkzeug mitliefert — *was diese Prüfung nicht gesehen hat*. Wer nur die Funde liest, hält sonst für geprüft, was gar nicht geprüft wurde.

Die Oberfläche läuft im Browser, auf Deutsch und Englisch, und braucht auf Ihren Arbeitsplätzen keine Installation.

Alles auf einen Blick

Jede Funktion, jeweils in einem Satz

FUNKTION	WOGEGEN	WIE
Geräteverzeichnis	Vergessene Geräte	Jedes Gerät im Netz befragen, Hersteller und Dienste erfassen
Dienstbewertung	Offene Zugänge, Werkskennwörter, alte Systeme	Regelwerk übersetzt Fundstellen in Klartext samt Maßnahme
Veränderungserkennung	Heimliche Neuzugänge	Jeden Lauf mit dem vorherigen vergleichen
Netzwerkgeräte	Übernahme von Switch und Router	Verwaltungsoberflächen gesondert prüfen
Windows-Härtung	Diebstahl von Zugangsdaten im Netz	Über zwanzig Einstellungen je System prüfen
Linux-Härtung	Vergessene Server	Fernzugang, Konten, Updates, Firewall, Protokollierung
Benutzerverwaltung	Sprung zu Administratorrechten	Kennwortregeln, Dienstkonten, Delegation, LAPS
Zertifikatdienste	Ausweis auf fremden Namen	Vorlagen und Rechte der Ausstellungsstelle prüfen
Erreichbarkeit	Lücken im Bericht	Aufschlüsseln, warum ein System nicht antwortete
Namensköder	Mitschneiden von Anmeldungen	Nach erfundenen Rechnern fragen; wer antwortet, verrät sich
Köderdateien	Datendiebstahl, Verschlüsselung	Echte Tabellen zwischen echten Dateien, Zugriff meldet
Köderkonten	Verwertung gestohlener Daten	Konten, die es gibt, mit Kennwörtern, die nicht gehen
Konten-Überwachung	Kennwort-Raten, Rechteausweitung	Gescheiterte Anmeldungen, neue Verwalterrechte und neue Konten auswerten
Verdächtige Konten	Datendiebstahl mit übernommenem Konto	Konto mit Spur plus Zugriff auf eine echte Freigabe binnen 24 Stunden
Köderdienste	Erkundung, Ausbreitung	Offene Zugänge ohne Inhalt; jede Verbindung ist eine Suche
Geräteabgleich	Eingeschmuggelte Geräte	Geräteerkennung gegen Adresse und Bestand halten
Selbsttest	Blinde Überwachung	Jede Falle auf Knopfdruck auslösen
Spurensuche	Eingerichteter Eindringling	Autostart, Verbindungen, Konten gegen den Normalzustand
Außenseite	Selbst geöffnete Rückwege	Freigaben des Routers abfragen und vergleichen
Adresschronik	Fehlende Beweislage	Öffentliche Adresse fortlaufend mitschreiben
Webzugriffe	Einbruch über den Dienst im Internet	Liste des Reverse Proxys live mitlesen, Scanner rot, Anmeldeversuche melden
Ortung	Ratlosigkeit nach der Meldung	Adresstabelle des Switches lesen, Dose benennen
Alarm	Übersehene Meldungen	E-Mail oder Webhook, zusammengefasst
Berichte	Unlesbare Rohdaten	Befund, Auswirkung, Maßnahme — und was ungeprüft blieb

Wo unsere Arbeit endet — und was daneben nötig bleibt

Damit Sie wissen, worauf Sie sich verlassen können

Sicherheit entsteht in Schichten, nicht aus einem Produkt. Wir sind eine davon — eine, die es in den meisten Betrieben bisher gar nicht gibt. Hier steht, wo unsere Schicht aufhört und welche daneben gehört. Wer Ihnen an dieser Stelle nichts sagt, hat entweder nicht darüber nachgedacht oder verkauft Ihnen ein Gefühl.

Der Virenschutz bleibt Ihre erste Reihe

Schadsoftware, die auf einem einzelnen Rechner sitzt, ohne einen Zugang zu öffnen und ohne im Netz zu suchen, gehört dorthin. Wir sind die Stufe danach — und prüfen zugleich, ob diese erste Reihe überhaupt steht: läuft der Echtzeitschutz, sind die Signaturen aktuell, hat jemand ihn abgeschaltet.

- **Phishing entscheidet sich am Menschen.** Ob jemand auf einen Anhang klickt, kann kein Netzwerkwerkzeug verhindern. Dafür sind wir die Stufe danach: Wir merken, was der Klick ausgelöst hat — die Verbindung nach draußen, das neue Konto, den Zugriff auf Dateien, die niemand hätte öffnen dürfen.
- **Wir bewerten Konfiguration und Erreichbarkeit** — also das, was sich abstellen lässt. Auf Wunsch kommt eine Suche gegen bekannte Schwachstellen dazu: ein zusätzliches Prüfprogramm (Nuclei) auf dem Hub, dessen Treffer wir in Befunde übersetzen, bündeln und nach der Wichtigkeit Ihrer Geräte gewichten. Sie läuft im Haus; Prüfungen, die einen Server im Internet einbeziehen würden, sind abgeschaltet.
- **Kennwörter prüfen wir dort, wo es zählt:** in den Regeln der Benutzerverwaltung — Mindestlänge, Sperrung nach Fehlversuchen, Sonderregeln, die die Vorgabe unterlaufen. Die Kennwörter Ihrer Mitarbeiter selbst sehen wir nicht, und das ist so gewollt.
- **Wir arbeiten in Ihrem Netzsegment.** Was hinter einem weiteren Router liegt, ist ein eigenes Netz und braucht dort einen eigenen Zugang — bei mehreren Standorten planen wir das mit ein.
- **Befunde werden einzeln eingestuft** und nach der Wichtigkeit Ihrer Geräte gewichtet: Derselbe Fehler wiegt auf dem Warenwirtschaftsserver schwerer als auf einem Testrechner. Wo mehrere Einstellungen zusammen einen durchgehenden Angriffsweg ergeben, benennen wir ihn ausdrücklich als solchen.
- **Ein Bericht beschreibt einen Zeitpunkt.** Deshalb ist der Vergleich mit dem letzten Lauf fest eingebaut — Sicherheit ist nichts, was man einmal feststellt, sondern etwas, das man beobachtet.

Und ein Punkt, der uns wichtig ist: **Wir gehen mit empfindlichen Geräten vorsichtig um.** Steuerungen, Medizintechnik, Drucker und unterbrechungsfreie Stromversorgungen vertragen aktive Prüfungen oft

nicht. Solche Geräte werden vor dem ersten Lauf ausgenommen — sie stehen auf einer Liste, die nie gescannt wird.

Warum es Ihr Haus nicht verlässt

Die Entscheidung hinter der Bauweise

Bei jeder Auswertung entsteht etwas, das man nicht leichtfertig aus der Hand gibt: eine vollständige Landkarte Ihres Netzes. Alle Adressen, alle Rechnernamen, alle Betriebssysteme, alle offenen Dienste, alle Softwareversionen. Wer sie hat, weiß über Ihr Netz mehr als die meisten Ihrer Mitarbeiter.

Deshalb gibt es in diesem Werkzeug keine Cloud, keine Künstliche-Intelligenz-Schnittstelle und keine Telemetrie. Die Auswertung läuft auf Ihrem Gerät, in Ihrem Netz. Es verlässt kein Byte Ihren Betrieb.

Das hat einen Preis, den wir offen nennen: Die Bewertung folgt einem Regelwerk, das Menschen geschrieben haben, und nicht einem Modell, das Zusammenhänge selbst findet. Dafür ist jeder Befund nachvollziehbar — es steht immer dabei, woran er erkannt wurde.

Für die Prüfung wird auf Ihren Arbeitsplätzen nichts installiert: Das Werkzeug läuft auf einem Gerät und fragt von dort aus, bedient wird es im Browser. Die laufende Überwachung kennt einen Sensor, der auf einem Rechner mitläuft — Option, nicht Pflicht, und Sie wählen, auf welchen. Was er meldet und was er nie tut, steht vollständig in einem eigenen Blatt.

Alle Aussagen in diesem Dokument beschreiben Funktionen, die im Werkzeug vorhanden sind. Was geplant, aber noch nicht vorhanden ist, ist als solches gekennzeichnet — unter „Wo unsere Arbeit endet“ und nirgends sonst.