

Wissen, was in Ihrem Netzwerk passiert

Sicherheitsanalyse und Angriffserkennung für den Mittelstand. Ohne Mustererkennung, alles in einer Software. Vollständig in Ihrem Haus. Ohne Cloud.

Die meisten Betriebe wissen nicht genau, welche Geräte in ihrem Netzwerk hängen. Kein Vorwurf — über Jahre kommen Drucker, Kameras, Steuerungen, Telefonanlagen und Testrechner dazu, und niemand führt Buch. Genau diese Lücke nutzen Angreifer: nicht mit spektakulären Methoden, sondern mit dem vergessenen Gerät, dem Werkskennwort und dem Dienst, von dem niemand mehr wusste, dass er läuft.

Drei Aufgaben, eine Lösung

01 – SEHEN

Was ist überhaupt da?

Jedes Gerät im Netz, mit Hersteller, Betriebssystem und allen erreichbaren Diensten. Dazu die Bewertung: Was davon ist ein Risiko, was kann passieren, was ist zu tun.

02 – HÄRTEN

Wie ist es eingestellt?

Über zwanzig Prüfpunkte je Windows-Rechner, dazu Linux-Server, Benutzerverwaltung und die Geräte, die das Netz tragen — Switch, Router, Access Point.

03 – MERKEN

Ist jemand drin?

Fallen, die nur ein Angreifer auslösen kann: Dateien, die niemand öffnen dürfte, Dienste, die niemand ansprechen dürfte. Jeder Zugriff ist ein Treffer, kein Verdacht.

Was dabei geprüft und überwacht wird

- **Geräteverzeichnis** — jedes Gerät, jeder erreichbare Dienst
- **Veränderungen** — neues Gerät, neuer Zugang, neue Version
- **Offene Dienste** — Klartext-Anmeldungen, ungeschützte Datenbanken, Fernwartung, veraltete Verschlüsselung
- **Werkskennwörter** auf Weboberflächen
- **Windows-Härtung** — die Einstellungen, über die Zugangsdaten im Netz abgegriffen werden
- **Linux-Härtung** — Fernzugang, Konten, Updates, Firewall
- **Benutzerverwaltung** — Kennwortregeln, Dienstkonten, Delegation
- **Zertifikatdienste** — Ausweise auf fremde Namen
- **Namensköder** — erkennt das Mitschneiden von Anmeldungen
- **Köderdateien** zwischen Ihren echten Dateien — schlagen bei Datendiebstahl und Verschlüsselung an
- **Köderkonten** — melden, wenn gestohlene Zugangsdaten benutzt werden
- **Köderdienste** — jede Verbindung darauf ist eine Suche
- **Fremde Geräte** im Netz und umgeleiteter Verkehr
- **Spuren auf den Rechnern** — Autostart, Verbindungen, neue Konten
- **Türen nach außen** — Portfreigaben des Routers im Vergleich
- **Wer vor der Tür steht** — die Zugriffe auf Ihre Dienste im Internet live, Scanner rot, Anmeldeversuche gemeldet
- **Öffentliche Adresse** lückenlos mitgeschrieben — die Angabe, die eine spätere Auskunft beim Anbieter braucht
- **Portzuordnung am Switch** — vom Fund zum Anschluss in der Wand
- **Alarm** per E-Mail und Webhook, sofort

Was uns unterscheidet

- ✓ **Erkennt Angreifer, ohne sie zu kennen**
Firewall, Intrusion-Detection und Virenschutz erkennen Muster, die jemand vorher beschrieben hat, und laufen neuen Angriffen hinterher. Wir messen, was ein Angreifer im Netz tun muss: suchen, anmelden, Rechte holen, sich ausbreiten. So erkennen wir jeden, der sich in Ihrem Netz umsieht, egal womit. Und weil niemand sonst eine Falle anfasst, ist jede Meldung ein Befund.
- ✓ **Alles in einer Software**
Fallen, Anmeldeüberwachung, Sensor für Server, Eingriff am Switch-Port, an der Freigabe und am Router, Alarm- und Maßnahmenmatrix, Beweissicherung und Bestandsaufnahme. Wofür man sonst mehrere Produkte braucht, steckt hier unter einer Haube — mit einer Oberfläche und ohne eigenes Sicherheitspersonal.
- ✓ **Ihre Netzdaten verlassen den Betrieb nicht**
Keine Cloud, keine KI-Schnittstelle, keine Telemetrie, keine Updates über das Internet. Geräteverzeichnis, Protokolle und Vorfallsakten bleiben auf Ihrem Gerät. Nach außen gehen nur Ihre Alarmmeldungen, die Lizenzprüfung und bei einem Angriff aus dem Internet die Herkunftsabfrage zur Adresse des Angreifers.
- ✓ **Die Prüfung installiert nichts**
Das Werkzeug läuft auf einem Gerät und fragt von dort. Bedient wird es im Browser, auf Deutsch und Englisch. Nur die laufende Überwachung kennt einen Sensor, der auf einem Rechner mitläuft — Option, nicht Pflicht, und Sie wählen, auf welchen.

- ✓ **Berichte, die jemand lesen kann**
Kein Rohdatenexport, sondern Befund, Auswirkung und die Maßnahme, die jemand morgen umsetzen kann — nach Dringlichkeit sortiert und nach der Wichtigkeit Ihrer Geräte gewichtet.

- ✓ **Rücksicht auf empfindliche Geräte**
Steuerungen, Medizintechnik, Drucker und USV vertragen aktive Prüfungen oft nicht. Solche Geräte nehmen wir vor dem ersten Lauf aus.

Wenn es ernst wird

- **Alarm** per E-Mail, Webhook oder Push-Nachricht — mit täglicher Bestätigung, dass die Überwachung läuft. Bleibt sie aus, wissen Sie es.
- **Alle Eingriffe ab Werk ausgeschaltet** — gemeldet wird immer, eingegriffen erst, wenn Sie es freigeben
- **Sitzung kappen, Switch-Port abschalten** — mit einstellbarer Frist, und jeder Eingriff hat einen Rückweg in der Oberfläche
- **Internet trennen** — der grobe Hebel, für den Fall, dass alles andere zu spät kommt
- **Vorfallsakte** bei jedem Fund, angelegt vor dem Eingriff: Sitzungen, ARP-Tabelle, angemeldete Konten
- **Übernommene Konten** — welche Ordner und Dateien sie geöffnet, geändert oder gelöscht haben
- **Beweissicherung mit Prüfsummen** — jede Sicherung mit der vorherigen verkettet, nichts lässt sich unbemerkt ändern
- **Zwei Berichte** aus einer Sicherung — einer für die Geschäftsleitung, einer für die IT
- **Herkunft eines Angreifers** aus dem Internet: Netzbetreiber, Land und Abuse-Kontakt

So läuft es ab

01 – VORGESPRÄCH

Was ist geschäftskritisch, was darf nicht angefasst werden? Daraus entsteht die Liste der Ausnahmen vor dem ersten Scan.

02 – ANALYSE

Analyse des Netzwerks, Bericht mit Befunden und Maßnahmen, gemeinsame Durchsprache. Sie bekommen keine Datei, sondern eine Erklärung.

03 – UMSETZUNG

Sie in eigener Regie oder ich im Auftrag — je nachdem, wie viel Ihre eigene IT übernehmen will.

04 – ÜBERWACHUNG

Auf Wunsch: Fallen, Alarmierung, Sensor auf den Servern, die Sie benennen, und festgelegt, wo der Hub selbst eingreifen darf.

Was Sie bereitstellen

- **Windows:** aktiviertes Remoteverwaltungs-Interface (WinRM) und ein Prüfkonto mit Leserechten — meist per Gruppenrichtlinie für alle Rechner
- **Linux:** ein SSH-Zugang mit Schlüssel, auf den Prüfbefehl beschränkt
- **Ein Rechner für die Auswertung** — ein Kleinrechner unter Linux, ein kleiner Server oder eine virtuelle Maschine genügt
- **Eine schriftliche Freigabe** des Inhabers für das zu prüfende Netz

Sämtliche Abfragen sind lesend. Es wird nichts verändert, nichts installiert und nichts abgelegt. Die eine Ausnahme ist der Sensor der laufenden Überwachung — und er kommt nur auf die Rechner, die Sie dafür benennen.

Was der Hub nicht leistet

- **Kein Ersatz für den Virenschutz**
Für Schadsoftware auf einem Arbeitsplatz ist ein etabliertes Schutzprogramm zuständig. Der Hub ergänzt es um das, was es nicht sieht, und prüft, ob es läuft.
- **Kein Blick in Inhalte**
Wer wann mit wem spricht, ja. Was dabei übertragen wird, nicht. Den Verkehr zwischen zwei fremden Geräten sieht der Hub nur über einen Spiegelport am Switch.
- **Kein Konto ohne Spur**
Wer mit einem erbeuteten Kennwort nur die Ordner öffnet, die dieses Konto immer öffnet, sieht aus wie der Mitarbeiter selbst. Das Verhalten jedes Mitarbeiters zu bewerten, tut der Hub bewusst nicht.
- **Eine Prüfung ist eine Momentaufnahme**
Sicherheit entsteht durch Wiederholung. Deshalb gehören Veränderungserkennung und Zeitplan dazu — und auf Wunsch die laufende Überwachung.

Ein Angreifer muss suchen, bevor er etwas findet. Wir sorgen dafür, dass er dabei über etwas stolpert — und dass Sie es erfahren, solange Ihre Daten noch da sind.