

**GEGENÜBERGESTELLT**

Wo der Unterschied zum üblichen Sicherheitsscan liegt

Werkzeuge, die offene Dienste finden, gibt es reichlich, und die Erhebung machen sie gut — der Hub benutzt selbst eines davon. Was es nicht zu kaufen gab, ist das, was danach kommt: eine Auswertung, die für die Prüfung ohne Agenten auskommt, das Haus nicht verlässt, empfindliche Geräte in Ruhe lässt, weiß, welches Gerät Ihr Geschäft trägt — und im Ernstfall nicht nur meldet, sondern handelt. Links, wie eine Prüfung üblicherweise abläuft, ob mit einem gekauften Scanner oder als beauftragter Test. Rechts, wie der Hub arbeitet.

	Übliche Prüfung	AgenticSecurityHub
Prüfung und Erkennung	Schwachstellenscanner und Einbruchserkennung als zwei Produkte	Schwachstellenprüfung und Angriffserkennung in einem Gerät
Wie Angreifer erkannt werden	gar nicht — oder per Signaturvergleich, der neue Angriffe übersieht	Fallen und Verhaltensregeln statt Signaturen: Wer einen Köder berührt, hat dort nichts zu suchen
Windows und Linux	Liste von Schwachstellennummern	Härtungsprüfung je System, mit konkreter Empfehlung je Befund
Software auf den Rechnern	Agent je Arbeitsplatz, muss gepflegt werden	keine für die Prüfung; ein Sensor nur dort, wo Sie ihn wollen
Wo die Auswertung liegt	beim Anbieter, oft außerhalb der EU	auf Ihrer Hardware, ohne Verbindung nach außen
Empfindliche Geräte	werden mitgescannt, Störung möglich	vorab erfasst und ausgenommen
Gewichtung der Befunde	allgemeine Punktzahl je Schwachstelle	nach der Rolle des Geräts in Ihrem Betrieb
Form des Ergebnisses	Rohdaten oder Zahlenwert	Beleg, Auswirkung und Maßnahme im Klartext
Netzwerkgeräte	Switches und Access Points fallen oft durchs Raster	eigene Prüfung dafür, dazu der Port je Gerät
Zwischen zwei Läufen	nichts, bis zum nächsten Termin	Veränderungserkennung und laufende Überwachung
Fehlalarmmeldungen	gehen im Ereignisprotokoll unter	vom Domain Controller und den Sensoren gesammelt, Kennwortraten wird gemeldet
Übernommene Konten	fallen erst auf, wenn der Schaden da ist	Konto mit Spur an echten Daten wird gemeldet, samt Ordnern und Dateien
Im Angriffsfall	eine Meldung, wenn überhaupt	auf Wunsch automatisch: Dateifreigabe-Sitzung trennen, Netzwerkdose abschalten, Internet trennen
Alarmierung	Mail oder Konsole des Anbieters	E-Mail und Webhook parallel — Teams, Slack, Mattermost, Telegram, ntfy, Ticketsystem
Forensik	von Hand, wenn der Vorfall längst vorbei ist	automatische Vorfallsakte, angelegt vor dem Eingriff
Protokollierung und Beweise	Protokolle mit Lücken, nachträglich änderbar	jeder Fund protokolliert, nichts gelöscht, Sicherungen verkettet mit Prüfsummen
Fällt die Überwachung aus	merkt es oft niemand	Tagesdiagnose per Mail, auf Wunsch ein zweiter Hub als Rückfall
Betrieb ohne Internet	meist nicht möglich	möglich — die Lizenz wird einmalig aktiviert