

AgenticSecurityHub — Bedienungsanleitung

Diese Anleitung beschreibt die Arbeit mit der Weboberfläche des Hubs: was auf welcher Seite steht, was die Knöpfe tun und worauf im Alltag zu achten ist. Die Einrichtung — Installation, Zugänge zu Router, Switch und Domäne, die Sensoren auf Ihren Servern — übernehmen wir; sie ist nicht Teil dieser Anleitung.

Die Oberfläche ist auf Deutsch und Englisch umschaltbar (oben rechts). Begriffe stehen hier so, wie sie auf dem Bildschirm erscheinen.

1. Wozu der Hub da ist

Der Hub beantwortet drei Fragen über Ihr Netz:

1. **Was steht darin?** — jedes Gerät mit Hersteller, Betriebssystem und erreichbaren Diensten.
2. **Wo ist es angreifbar?** — Befunde mit Beleg, Auswirkung und dem nächsten Schritt.
3. **Ist gerade jemand drin?** — Fallen, die nur ein Angreifer auslöst, und die Auswertung von Anmeldungen und Zugriffen.

Alles läuft in Ihrem Haus. Die Bewertung stammt aus einem festen Regelwerk, nicht aus einer Auswertung im Internet.

2. Anmelden und Aufbau der Oberfläche

Die Oberfläche öffnen Sie im Browser unter der Adresse, die wir bei der Einrichtung festgelegt haben. Jede Seite verlangt eine **Anmeldung**.

Zusätzlich ist festgelegt, **von welchen Rechnern aus** etwas ausgelöst werden darf — Scan starten, Erkennung abschalten, Einstellungen ändern. Von anderen Rechnern aus lässt sich weiterhin alles ansehen, aber nichts anstoßen. Gerät ein Kennwort in falsche Hände, kann der Betreffende damit sehen, aber nicht eingreifen.

Kennwort vergessen? Es gibt keine Wiederherstellung; ein neues wird am Hub selbst gesetzt. Sprechen Sie uns an.

Oben rechts steht immer, wann der Bestand zuletzt erhoben wurde und welche **Wachen** gerade laufen. Steht dort eine Wache in Rot, ist sie eingeschaltet, läuft aber nicht — das ist der Zustand, der von außen aussieht wie ein laufender Schutz.

Die Seitenleiste ist in zwei Teile gegliedert:

Bereich	Seiten
Analyse — wie es um Ihr Netz steht	Übersicht, Geräte, Schwachstellen, Systemhärtung, Netzwerkgeräte, Portzuordnung am Switch, Persistenzspuren, Perimeter, Active Directory, Bestandsänderungen
Überwachung — was gerade passiert	Angriffserkennung, ARP-Überwachung, Fehlanmeldungen, Agenten, Agentenbestand, Webzugriffe, Angriffsprotokoll, Verbindungen, Vorfallsakten, Forensik, Einstellungsprotokoll

Dazu **Berichte**, **Lizenz**, **Einstellungen** und **Hilfe**.

3. Der übliche Ablauf der Analyse

1. **Einstellungen** → **Zu prüfendes Netz**. Welches Netz abgefragt wird, welche Geräte **nie** gescannt werden dürfen und welche geschäftskritisch sind. Die Netze, in denen der Hub selbst steckt, stehen als Vorschlag darunter.
2. **Übersicht** → **Scan starten**. Das Netz wird abgesucht; jedes Gerät kommt ins Inventar und wird bewertet. Ein erster Lauf über ein ganzes Netz dauert je nach Tiefe Minuten bis Stunden.
3. **Geräte** zeigt, was gefunden wurde: Betriebssystem, offene Dienste, wann zuletzt gesehen.
4. **Schwachstellen** ordnet die Befunde nach Schwere. Jeder Befund nennt den Beleg, die Auswirkung und den nächsten Schritt.
5. **Systemhärtung** prüft Windows- und Linux-Rechner von innen: Konten, Dienste, Verschlüsselung, veraltete Verfahren.
6. **Bestandsänderungen** vergleicht mit dem letzten Lauf. Ein neues Gerät oder ein neu geöffneter Zugang fällt hier auf.

Empfindliche Geräte — Steuerungen, Medizintechnik, Alarmanlagen, ältere Drucker — gehören in Schritt 1 auf die Ausnahmeliste. Sie werden dann nie aktiv geprüft.

Regelmäßig statt einmal

Ein Bericht von vor drei Monaten beschreibt ein Netz, das es so nicht mehr gibt. Unter **Einstellungen** → **Zeitgesteuerte Läufe** lassen sich Scan, Windows- und Linux-Härtung, Perimeter, Active Directory und Netzwerkgeräte täglich oder wöchentlich zu fester Uhrzeit legen. Ein Lauf, der wegen eines Neustarts ausfällt, wird nachgeholt; ein überfälliger steht rot in seiner Karte.

Die weiteren Analyseseiten

Seite	Was dort steht
Netzwerkgeräte	Prüfung von Switches, Routern und Access Points über ihre Verwaltungsoberflächen
Portzuordnung am Switch	zu jedem Gerät der Switch-Port, an dem es hängt — aus der Adresse wird ein Anschluss, bei beschrifteten Ports gleich der Raum. Dazu Adressen, die der Switch kennt und das Inventar nicht, und die Zahl freier Ports.
Persistenzspuren	was seit dem letzten Lauf auf einem Rechner dazugekommen ist: ein Programm mit Verbindung nach draußen, ein neuer Dienst, ein neues Konto
Perimeter	die Portfreigaben Ihres Routers, der vollständige Bestand und jede Veränderung; dazu die öffentliche Adresse im Zeitverlauf
Active Directory	Kennwortregeln, veraltete Konten, Dienstkonten, Zertifikatvorlagen

Bei der **Portzuordnung** steht in jeder Zeile, wie sicher sie ist (Spalte **Güte**). Hängen an einem Port viele Geräte — ein weiterer Switch, ein Access Point, ein Virtualisierungsserver —, ist die Angabe eine Richtung, keine Ortung; solche Ports sind als **Sammelport** gekennzeichnet. Geräte im WLAN hängen an keiner Dose; sie stehen am Port des Access Points.

Öffentliche Adresse im Zeitverlauf (Seite Perimeter): Fällt ein Vorfall erst Wochen später auf, muss für eine Auskunft beim Anbieter belegbar sein, welche Adresse Ihr Anschluss damals hatte. Das Feld beantwortet die Frage rückwirkend — und sagt dazu, ob der Zeitpunkt in einem tatsächlich beobachteten Abschnitt liegt oder in einer Lücke zwischen zwei Läufen.

4. Die Überwachung

Angriffserkennung

Die zentrale Seite der Überwachung. Dort stehen

- die **Wachen** — die Fallen, die dauerhaft laufen, jede mit eigenem Schalter. Sie bleiben eingeschaltet, auch über einen Neustart hinweg;
- die Zugriffe auf die Köder, mit Gerät, Konto, Adresse und — wenn die Portzuordnung eingerichtet ist — dem Switch-Port;
- unter **Fileshares** → **Verdächtige Konten** die Konten mit einer eindeutigen Spur und die Freigaben, auf denen sie in den letzten 30 Tagen waren;
- die **Maßnahmen** und ihre **Steuerung** (Abschnitt 5);
- **Probealarm senden** (Abschnitt 6).

Ordner und Dateien abholen fragt bei einem verdächtigen Konto die Dateiserver, welche Ordner und Dateien es geöffnet, geändert oder gelöscht hat. **Konto nachschlagen** holt dieselbe Liste für jedes beliebige Konto, über bis zu 30 Tage — so weit, wie das Protokoll des Dateiservers zurückreicht.

Der Selbsttest gehört dazu. Ein sauberes Netz und eine kaputte Erkennung sehen gleich aus: leere Liste. Der Selbsttest spielt den Angreifer und weist nach, dass die Falle anschlägt. Ohne ihn bedeutet ein leeres Ergebnis nichts.

Weitere Überwachungsseiten

Seite	Was dort steht
ARP-Überwachung	welche Hardware hinter welcher Adresse steckt, und jeder Wechsel. Meldet sich hinter dem Router andere Hardware, bleibt der Fund stehen, bis ihn jemand mit Als richtig übernehmen quittiert — etwa nach einem Routertausch.
Fehlanmeldungen	gescheiterte Anmeldungen am Domain Controller und an den Servern. Oben steht, ob die Aufzeichnung am Domain Controller eingeschaltet ist; erst dann ist eine leere Tabelle Ruhe.
Agenten / Agentenbestand	die Sensoren auf Ihren Servern: wer meldet, wer schweigt, welche Fassung — und welche bekannten Rechner noch keinen Sensor haben
Webzugriffe	jede Anfrage an Ihre Dienste im Internet, live; Auffälliges rot, mit einer Deutung im Klartext. Rechts oben CSV und PDF zum gesetzten Filter.
Angriffsprotokoll	alle Funde aller Verfahren in einer Tabelle — mit Zeitpunkt, Gerät, Switch-Port, Ampel und Begründung, darüber die Lage der letzten 24 Stunden. Die Seite für die Frage: Was war heute Nacht?
Verbindungen	wer wann mit wem gesprochen hat, sofern ein Spiegelport eingerichtet ist — ohne Inhalt
Vorfallsakten	was im Augenblick eines Fundes festgehalten wurde (Abschnitt 7)
Forensik	was der Hub nach einem Fund zusätzlich gesichert hat (Abschnitt 7)
Einstellungsprotokoll	wer wann von wo aus was am Hub verstellt hat (Abschnitt 8)

Schweigt ein Sensor, fragt der Hub den Rechner an. Antwortet der Rechner, läuft er ohne Sensor — das wird gemeldet, denn ein Angreifer schaltet als Erstes den Wächter ab. Antwortet er nicht, ist der Rechner aus, und das ist keine Meldung wert.

Wie ernst ein Fund ist

Jeder Fund trägt eine von vier Stufen: **erklärt, auffällig, hoch, kritisch** — und seine Begründung im Klartext. Umstände wie ein unbekanntes Gerät oder ein Zeitpunkt außerhalb der Geschäftszeiten heben die Stufe; ein Zugriff von außerhalb Ihres Netzes hebt sie stärker. Läufe, die der Hub selbst angekündigt hat, fallen auf **erklärt** zurück und wecken niemanden.

Ab welcher Stufe ein Verfahren **meldet** und ab welcher es **eingreift**, steht unter **Einstellungen** → **Alarmmatrix**. Protokolliert wird unabhängig davon immer alles; die Matrix entscheidet nur, was darüber hinaus geschieht. Die Voreinstellung haben wir mit Ihnen abgestimmt — ändern Sie sie nur nach Rücksprache.

5. Eingreifen

Auf der Seite **Angriffserkennung** stehen die einzigen Stellen der Oberfläche, die etwas an Ihrem Netz verändern. Sie sind nach Härte geordnet, und jede trifft ein **Gerät**, kein Konto:

Maßnahme	Wirkung
Sitzung trennen	beendet die Verbindung zur Freigabe. Der schwächste Eingriff — eine neue Sitzung ist schnell aufgebaut.
Switch-Port abschalten	nimmt das Gerät vom Netz. Hängt an dem Port ein Verteiler, trifft es alles dahinter; die Vorschau nennt vorher die Zahl.
Internetverbindung trennen	nimmt allen den Weg nach draußen — samt Telefonie, Cloud, Fernwartung und den Meldewegen des Hubs.

Bei der dritten Maßnahme legt ein Umschalter fest, ob nur die **Verbindung getrennt** wird (mild: im Haus läuft alles weiter, der Anschluss kommt meist von selbst zurück) oder der **Router neu startet** (zwei bis fünf Minuten steht im Haus alles; dafür kann der Anschluss mit einer neuen öffentlichen Adresse zurückkommen). Ob die Adresse wirklich wechselt, entscheidet Ihr Anbieter; der Hub sieht nach und meldet das Ergebnis.

Wer beim Zugriff verbunden war, steht mit Konto, Rechnername und Adresse in der Zugriffstabelle; die passenden Knöpfe stehen in derselben Zeile.

Was von selbst passiert

Ab Werk greift der Hub nie von selbst ein. Gemeldet wird immer; eingeschaltet wird die Automatik unter **Angriffserkennung** → **Steuerung** → **Automatische Maßnahmen** — erst nachdem sie erprobt ist. Läuft ein angekündigter **Prüfbetrieb**, ruhen alle Maßnahmen, während weiter gemeldet wird.

Ein abgeschalteter Port geht nach einer einstellbaren Frist von selbst wieder an (Vorgabe 30 Minuten), allerdings nur innerhalb eines Zeitfensters zu Arbeitszeiten — läuft die Frist nachts ab, kommt der Port zum nächsten Arbeitsbeginn zurück.

Zurücknehmen

Neben jedem Eingriff steht ein Knopf, dazu **Alle Eingriffe zurücknehmen**. Eine gekappte Sitzung braucht nichts; der Rechner verbindet sich selbst neu.

Das Notfallblatt ausdrucken. Unter **Hilfe** steht das *Notfallblatt*: wie Switch-Port und Internetverbindung **ohne** den Hub wieder in Betrieb gehen. Es gehört ausgedruckt in den Serverschrank — fällt der Hub aus, ist genau dieser Bildschirm weg.

6. Alarmierung

Unter **Einstellungen** → **Alarmierung**: E-Mail, Webhook (etwa Teams, Slack, Telegram, ntfy) oder beides. Ohne Alarmweg steht ein Fund nur in der Oberfläche — und wer sie nicht offen hat, erfährt nichts. **Beide Wege zusammen** sind der empfohlene Betrieb: Fällt einer aus, kommt die Meldung trotzdem an.

- **Testnachricht senden** prüft den Weg. Sie kommt bewusst leise.
- **Probealarm senden** (Seite Angriffserkennung) kommt mit derselben Dringlichkeit und demselben Ton wie ein echter Fund — die Antwort auf die Frage, ob das Telefon nachts klingelt. Ausgelöst wird dabei nichts.

Was meldet: Zugriffe auf Köder, Anmeldungen mit Köderkonten, Angriffe auf die Namensauflösung, ein Router mit anderer Hardware, umgeleiteter Verkehr, Eingriffe — auch selbst ausgelöste — und die Ergebnisse der Automatik.

Was nicht meldet: Befunde aus Scans und Prüfungen, eine neue Portfreigabe, ein neues Gerät im Netz. Das sind Zustände, keine Vorfälle; sie stehen in Oberfläche und Bericht, aber sie wecken niemanden nachts.

Tagesdiagnose

Die Alarmierung meldet, was der Hub sieht. Fällt er selbst aus, meldet er nichts mehr — und das sieht aus wie eine ruhige Woche. Unter **Einstellungen** → **Zeitgesteuerte Läufe** lässt sich deshalb eine **Tagesdiagnose** planen: offene Punkte, Zustand der Wachen, Speicherplatz, Temperatur und letzte Sicherung. Sie kommt auch, wenn alles in Ordnung ist. **Bleibt sie aus, stimmt etwas nicht.**

7. Nach einem Vorfall

Vorfallsakten

Bei jedem Fund legt der Hub eine Akte an — **vor** jedem Eingriff: offene Sitzungen, die Zuordnung von Adressen und Geräten, wer am verdächtigen Gerät angemeldet ist. Was darin steht, lässt sich nachträglich nie wieder erheben. Der Knopf auf dieser Seite löscht deshalb nichts, sondern legt die Akten mit Zeitstempel beiseite.

Forensik

Nach jedem gemeldeten Fund sammelt der Hub zusätzlich das Große und Langsame: laufende Programme, Protokolle, Konfiguration und alles, was über die Quelle bekannt ist — bei einem Zugriff aus dem Internet auch Netzbetreiber, Land und den Missbrauchskontakt. Das läuft immer und lässt sich nicht abstellen. Zugangsdaten werden vorher entfernt.

Jede Sicherung trägt **Prüfsummen** und ist mit der vorherigen **verkettet**; keine lässt sich unbemerkt austauschen. Wer eine Sicherung weitergibt — an einen Gutachter, eine Versicherung, die Polizei —, gibt `pruefsummen.txt` mit; geprüft wird dort ohne den Hub.

Den jüngsten Kettenwert außer Haus notieren. Unten auf der Seite Forensik steht er. Ausgedruckt, in einer Mail, beim Steuerberater — es genügt, dass er woanders liegt. Damit lässt sich später belegen, dass keine Sicherung entfernt wurde.

Aus einer Sicherung entstehen **zwei Berichte**: einer für die Geschäftsleitung (was ist passiert, wie schlimm, was ist zu entscheiden, was wissen wir nicht) und einer für die IT. Wird der Platz knapp, sagt die Seite, dass weggetragen werden muss — von selbst gelöscht wird nichts.

8. Berichte, Aufräumen und Selbstschutz

Berichte

Jeder Prüflauf erzeugt einen Bericht, lesbar und als PDF: Zusammenfassung, Befunde nach Dringlichkeit, je Befund Beleg, Auswirkung und Maßnahme — und ein Abschnitt, was der Lauf **nicht** gesehen hat.

Aufräumen

Jede Karte mit Befunden trägt einen Leeren-Knopf, die Berichtsseite einen für alle Berichte, die Übersicht ganz unten einen für alles. Vor dem Löschen kommt eine Rückfrage mit der Anzahl.

Erhalten bleiben dabei mit Absicht die **Vergleichsstände** (sonst wäre der nächste Lauf wieder ein Erstlauf) und die **Chronik der öffentlichen Adresse**. Protokolle der Fallen werden nicht gelöscht, sondern beiseitegelegt: Nach einem Fehlalarm sind sie der Beleg, dass es einer war.

Wer hat am Hub etwas verstellt?

Das **Einstellungsprotokoll** zeigt jeden Handgriff an der Oberfläche mit Zeitpunkt, Konto und Adresse — auch abgewiesene Versuche. Es hat keinen Leeren-Knopf: Wer sich Zutritt verschafft hat, würde als Erstes die Zeile wegräumen, die ihn nennt.

Gemeldet wird, was die Erkennung schwächt — eine Wache anhalten, die Alarmmatrix ändern, eine Falle entfernen. Diese Meldung kommt auch bei eigenen Handgriffen. Das ist gewollt: Wer sie bekommt, ohne gerade am Hub zu sitzen, weiß genug.

9. Einstellungen — was dort steht

Die Einstellungen sind in Reiter gegliedert. Der Reiter **Betrieb** trägt eine Zahl, wenn Punkte offen sind.

Karte	Wofür
Zu prüfendes Netz	Netz, Ausnahmen, geschäftskritische Geräte
Zugang zum Router, Geräteliste des Routers	Portfreigaben, öffentliche Adresse, welche Geräte ins Haus gehören
Zugang zur Domäne	Prüfung des Active Directory, Abholen der Fehlanmeldungen
Anmeldung, Adresse der Weboberfläche, Verschlüsselung der Oberfläche (HTTPS)	wer sich anmeldet, von wo aus bedient werden darf
Überwachung, Köderfreigabe auf dem Hub, Köderkonten im Active Directory	die Fallen
Portzuordnung am Switch, Trennen am Switch, Spiegelport	Ortung und Eingriff am Switch
Alarmierung, Alarmmatrix	wohin gemeldet wird, ab wann gemeldet und eingegriffen wird
Betriebsbereitschaft	was der Hub gerade kann — und was ihm fehlt
Zeitgesteuerte Läufe	Prüfläufe und Tagesdiagnose
Webzugriffe (Reverse Proxy)	ob Zeilen angenommen werden und wie lange sie bleiben
Einstellungen sichern und übertragen	alle Einstellungen als verschlüsselte Datei

Betriebsbereitschaft

Eine Prüfung, die nicht laufen kann, sieht aus wie eine, die nichts gefunden hat: leer. Die Karte geht deshalb jede Voraussetzung einzeln durch — Zugang zum Router, Trennen am Switch, Aufzeichnung am Domain Controller, Herzschlag der Sensoren, laufende Wachen — und sagt bei jeder, die fehlt, was zu tun ist. Keine Gesamtnote.

Schauen Sie nach jeder Änderung im Netz hier vorbei.

Einstellungen sichern

Exportieren lädt alle Einstellungen als eine Datei herunter, immer verschlüsselt. Die Passphrase steht nirgends auf dem Hub und gehört in Ihren Kennwortsafe; der Export wird gemeldet, weil mit der Datei Zugangsdaten das Haus verlassen. **Importieren** zeigt vorher, was sich ändert, und legt den bisherigen Stand zum Zurückholen ab.

10. Was der Hub nicht sieht

- **Verkehr zwischen zwei anderen Geräten** — nur über einen Spiegelport am Switch.
- **Geräte in einem anderen Netzsegment** hinter einem weiteren Router.
- **Schadsoftware auf einem Arbeitsplatz** — das ist Sache des Virenschutzes.
- **Ob eine Schwachstelle im konkreten Fall ausnutzbar ist** — geprüft wird der Zustand, nicht der Einbruch.
- **Ein übernommenes Konto ohne jede Spur**, das nur seine gewohnten Ordner öffnet.

Was Sie selbst im Blick behalten sollten

- **Die Tagesdiagnose lesen.** Bleibt sie aus, ist der Hub ausgefallen oder kann nicht mehr senden.
- **Den Probealarm einmal auslösen** — und prüfen, ob er ankommt, auch nachts.
- **Das Notfallblatt ausgedruckt** im Serverschrank aufbewahren.
- **Den Kettenwert der Forensik** gelegentlich außer Haus notieren.
- **Nach Änderungen im Netz** — neuer Router, neuer Switch, neuer Server — die Betriebsbereitschaft ansehen und uns Bescheid geben.

RB-COMPUTERSERVICE · Roman Brunetti · Elbestraße 8c, 90453 Nürnberg · 0911 6320968 · info@rb-computerservice.de