

SECURITY AWARENESS · VORTRAG

Hack or get Hacked

Erhalte die Kontrolle zurück.

Henry Werner · Security Awareness Enthusiast · Speaker
Sales Engineer bei Enginsight



**Ich liefere keine Pizza.
Ich liefere Leidenschaft.**

Ich zeige dir nicht, wie man hackt – ich zeige dir, wie man Sicherheit versteht.

ÜBER MICH

Kein Experte, sondern Entdecker

Lernen nie aus

Ich behaupte nicht, allwissend zu sein. In der IT-Security lernt man nie aus, und genau das treibt mich an. Ich suche den Austausch auf Augenhöhe, liebe es, neue Dinge zu lernen und diese Begeisterung mit einer großen Portion Leidenschaft zu teilen.

Meine Mission

Ob ich im Lieferdienst-Outfit auf die Bühne gehe oder komplexe Gadgets erkläre: Meine Mission ist es, Menschen für Technik zu sensibilisieren, ohne sie zu belehren. Hauptberuflich bringe ich diese Passion als Sales Engineer bei Enginsight ein.

WORUM GEHT ES HEUTE?

Wir wechseln die Perspektive

Warum klicken wir auf Phishing-Mails? Wie einfach ist es wirklich, in ein Netzwerk einzudringen?

Live und mit viel Humor zeige ich, wie Hacker denken und arbeiten. IT-Sicherheit nicht als theoretisches Hindernis, sondern als spannendes Katz-und-Maus-Spiel.

Sie werden Ihren Laptop danach mit anderen Augen sehen – und verstehen, wie Sie die Kontrolle zurückgewinnen.

Teil 1

Was das Internet über uns verrät

Teil 2

Die Werkzeugkiste – 15 Gadgets

Teil 3

Fazit – Kontrolle zurückgewinnen mit Enginsight

TEIL 1

Was das Internet über uns verrät

Viele Cyberangriffe beginnen nicht mit einem spektakulären Hack. Sie beginnen mit Informationen.

Fünf Fragen, die sich jeder Angreifer stellt

1

Welche Systeme
sind erreichbar?

2

Welche Technik
wird eingesetzt?

3

Welche Personen
arbeiten dort?

4

Welche
Infrastruktur
existiert?

5

Welche
Unternehmen
wurden bereits
Opfer?

Wichtig

Öffentlich sichtbar bedeutet nicht automatisch unsicher – und erst recht nicht, dass ein System getestet, verändert oder betreten werden darf. Die Beispiele dienen ausschließlich der Security Awareness und zeigen, warum Unternehmen ihre von außen sichtbare Angriffsfläche kennen sollten.

Shodan – die Suchmaschine für erreichbare Systeme

Was ist hier zu sehen?

Shodan durchsucht nicht primär Webseiteninhalte wie eine klassische Suchmaschine. Stattdessen erfasst es Informationen über Dienste und Geräte, die über das Internet erreichbar sind: IP-Adressen, Ports, verwendete Software, Protokolle und weitere technische Metadaten.

Warum kann das gefährlich sein?

Ein Angreifer muss nicht mehr jedes Unternehmen einzeln untersuchen. Suchmaschinen für Internet-Infrastruktur helfen, eine große Zahl öffentlich erreichbarer Systeme zu identifizieren und nach bestimmten Eigenschaften zu sortieren.

Awareness-Lernpunkt



Unternehmen sollten wissen, welche ihrer eigenen Systeme aus dem Internet sichtbar sind. Nicht benötigte Dienste sollten nicht öffentlich erreichbar sein. Exponierte Systeme gehören konsequent aktualisiert, überwacht und abgesichert.



Kameras & RTSP-Streams

Was zeigt das Beispiel?

Die Suche kombiniert geografische Informationen mit dem für Videostreaming häufig verwendeten RTSP-Dienst und dem Hinweis, dass Shodan ein Vorschaubild erfasst hat.

Wo liegt das Risiko?

Öffentlich erreichbare Kameras können Informationen über Gebäude, Produktionsbereiche, Arbeitszeiten, Personen oder physische Sicherheitsmaßnahmen preisgeben. Ein sichtbarer Treffer bedeutet nicht automatisch, dass die Kamera ohne Authentifizierung zugänglich ist.

Awareness-Lernpunkt



Kameras gehören normalerweise nicht direkt ins öffentliche Internet. Sichere Konfiguration, aktuelle Firmware, Netzwerksegmentierung, starke Authentifizierung und kontrollierte Fernzugriffe reduzieren das Risiko deutlich.



NAS-Systeme im Internet

Was zeigt die Suche?

Die Suche versucht, öffentlich erreichbare Webdienste anhand des Seitentitels „Synology DiskStation“ zu identifizieren.

Warum ist das relevant?

NAS-Systeme enthalten häufig zentrale Unternehmensdaten, Dokumente oder Backups. Ist eine Administrationsoberfläche öffentlich erreichbar, wird sie Teil der externen Angriffsfläche des Unternehmens.

Awareness-Lernpunkt



Administrative Oberflächen sollten nur dort erreichbar sein, wo das wirklich notwendig ist. MFA, Updates, Firewall-Regeln, sichere Fernzugänge und unabhängige Backups sind besonders wichtig.



Öffentlich sichtbare Login-Seiten

Was zeigt das Beispiel?

Shodan kann Weboberflächen unter anderem anhand ihres Seitentitels finden. Diese Suche zeigt Systeme, deren Titel das Wort „Login“ enthält.

Bedeutet ein Treffer eine Schwachstelle?

Nein. Eine Login-Seite allein ist keine Sicherheitslücke. Sie zeigt aber, dass eine Anmeldeoberfläche öffentlich erreichbar ist und damit grundsätzlich Teil der Angriffsfläche wird.

Awareness-Lernpunkt



MFA, sichere Passwörter, Schutz vor automatisierten Anmeldeversuchen, Monitoring und möglichst geringe öffentliche Exposition gehören zu den wichtigsten Schutzmaßnahmen.

OSINT Framework – digitale Spuren kombinieren

Was ist OSINT?

Open Source Intelligence bezeichnet die systematische Auswertung öffentlich zugänglicher Informationen. Das OSINT Framework sammelt dafür zahlreiche Werkzeuge und Datenquellen.

Wo entsteht die Gefahr?

Eine einzelne Information wirkt oft harmlos. LinkedIn, Social Media, Firmenwebseite, Presseartikel, Domains und andere Quellen können zusammen ein erstaunlich detailliertes Bild ergeben. Das erleichtert Social Engineering und gezieltes Phishing erheblich.

Awareness-Lernpunkt



Vor dem Veröffentlichen sollte man sich fragen: Welche Information gebe ich preis? Und was ergibt sich, wenn jemand diese Information mit zehn anderen Quellen kombiniert?

Reale Sicherheitsvorfälle

Was ist hier zu sehen?

Die Datenbank sammelt öffentlich bekannte Datenpannen, Cyberangriffe, Schwachstellen und weitere Sicherheitsvorfälle.

Warum ist das für Awareness wertvoll?

Cyber Risiken wirken schnell abstrakt. Reale Vorfälle zeigen, dass Unternehmen jeder Größe und unterschiedlichster Branchen betroffen sein können.

Awareness-Lernpunkt



IT-Sicherheit ist kein rein theoretisches Thema. Incident Response, Backups, Patchmanagement, Segmentierung, Mitarbeiterschulung und klare Verantwortlichkeiten müssen vorbereitet sein, bevor etwas passiert.

Ransomware weltweit

Was zeigt die Karte?

Ransomware.live sammelt Informationen zu öffentlich bekannt gewordenen bzw. von Ransomware-Gruppen beanspruchten Opfern. Die Karte visualisiert, wie international diese Form der Cyberkriminalität ist.

Was bedeutet ein Ransomware-Angriff?

Moderne Ransomware bedeutet häufig nicht nur verschlüsselte Dateien. Auch Datendiebstahl, Betriebsunterbrechung, Erpressung, Reputationsschäden und hohe Wiederherstellungskosten können dazugehören.

Awareness-Lernpunkt



Wiederherstellbare Backups, MFA, Segmentierung, aktuelle Systeme, Endpoint-Schutz und ein geübter Incident-Response-Prozess können im Ernstfall entscheidend sein.

Die Erpressung danach

Was ist hier zu sehen?

Ransomware.live veröffentlicht Beispiele dokumentierter Kommunikation zwischen Opfern bzw. deren Vertretern und Ransomware-Akteuren.

Warum ist das bemerkenswert?

Cyberangriffe enden nicht mit der technischen Kompromittierung. Danach beginnen psychologischer Druck, Zeitdruck, wirtschaftliche Entscheidungen und Erpressung. Zahlung oder Kommunikation garantieren nicht, dass Daten tatsächlich gelöscht werden.

Awareness-Lernpunkt



Ein Ransomware-Vorfall darf nicht improvisiert werden. Incident Response, Geschäftsführung, IT, Datenschutz, Rechtsberatung und ggf. Strafverfolgungsbehörden müssen koordiniert zusammenarbeiten.



Fallbeispiel: Akira

Warum dieses Beispiel?

Statt nur über „Ransomware-Gruppen“ zu sprechen, lässt sich hier anhand einer konkreten dokumentierten Kommunikation nachvollziehen, wie eine digitale Erpressung tatsächlich aussehen kann.

Das eigentliche Risiko

Hinter einer technischen Sicherheitslücke können plötzlich reale Menschen, Geschäftsentscheidungen, Fristen, finanzielle Forderungen und existenzielle Folgen stehen.

Awareness-Lernpunkt



Prävention ist wichtig. Genauso wichtig ist die Vorbereitung darauf, dass Prävention einmal nicht funktioniert. Ein Unternehmen benötigt deshalb einen belastbaren Notfallplan.

Kritische Infrastruktur als Open Data

Was zeigt die Karte?

FLOS visualisiert auf Grundlage von OpenStreetMap-Daten Stromnetze, Kraftwerke, Leitungen, Umspannwerke und teilweise detaillierte Infrastruktur.

Warum ein gutes Awareness-Beispiel?

Die Daten sind nicht automatisch geheim. Interessant wird, wie viele einzelne, öffentlich verfügbare Informationen miteinander kombiniert werden können. Genau dieser Aggregationseffekt ist ein zentraler Bestandteil von OSINT.

Awareness-Lernpunkt



Sicherheit bedeutet nicht, alle öffentlichen Informationen zu verstecken. Organisationen sollten aber verstehen, welche zusätzlichen betrieblichen Informationen sie selbst veröffentlichen und welches Gesamtbild daraus entstehen kann.

TEIL 2

Die Werkzeugkiste 15 Gadgets

Hardware, die ich zur Veranschaulichung nutze – was sie kann und warum Unternehmen sich mit solchen Angriffsszenarien beschäftigen sollten.

Auf einen Blick



WiFi Pineapple Pager



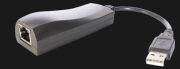
HackRF One + PortaPack



Flipper Zero



Plunder Bug



LAN Turtle



USB Rubber Ducky



Shark Jack



Pwnagotchi



O.MG Elite Kabel



O.MG Adapter



WiFi Pineapple Mk7



Bash Bunny



Packet Squirrel



Screen Crab



Key Croc

GADGET 1 / 15

WiFi Pineapple Pager

Ein eigenständiges, mobiles WiFi-Pentesting-Gerät. Es kann WLAN-Umgebungen analysieren und für autorisierte Security-Tests unterschiedliche WLAN-Angriffsszenarien simulieren.



Mobiles WiFi-Pentesting und WLAN-Reconnaissance.

Was ist die Gefahr?

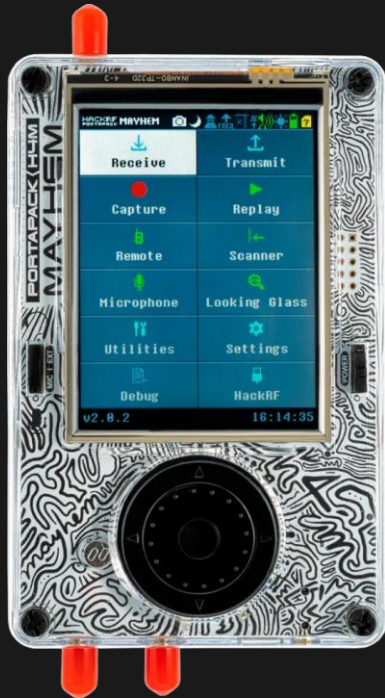
Ein Angreifer in Funkreichweite kann versuchen, sich als vertrauenswürdiges WLAN auszugeben, Verbindungen zu beeinflussen oder Informationen über WLAN-Geräte und Netzwerke zu sammeln.

Awareness-Lernpunkt

Bekannte WLAN-Namen sind kein Beweis dafür, dass man wirklich mit dem richtigen Netzwerk verbunden ist. WPA2/WPA3, Zertifikatsprüfung, sichere Unternehmens-WLANs und der Verzicht auf unkontrolliertes Auto-Join reduzieren das Risiko.

HackRF One + PortaPack

HackRF One ist ein Software Defined Radio, das Funksignale in einem sehr breiten Frequenzbereich empfangen und senden kann. Das PortaPack ermöglicht einen mobilen Betrieb.



Software Defined Radio für Funkanalyse.

Was ist die Gefahr?

Viele ältere Funkprotokolle wurden nicht mit moderner kryptografischer Sicherheit entwickelt. Je nach Technik können Signale analysiert, aufgezeichnet, nachgebildet oder gestört werden. Moderne Systeme mit kryptografischer Authentifizierung sind wesentlich widerstandsfähiger.

Awareness-Lernpunkt

„Funk“ bedeutet nicht automatisch „sicher“. Besonders bei Zugangssystemen, Sensorik, Fernbedienungen und älteren IoT-Komponenten sollte geprüft werden, ob tatsächlich Authentifizierung und Verschlüsselung eingesetzt werden.

Flipper Zero

Ein tragbares Multi-Tool, das unter anderem mit RFID, NFC, Sub-GHz-Funk und Infrarot arbeiten kann.



Multi-Tool für Funk, RFID, NFC und Infrarot.

Was ist die Gefahr?

Insbesondere ältere Zugangssysteme oder einfache Funkprotokolle speichern bzw. übertragen teilweise nur statische Kennungen. Solche Systeme bieten deutlich weniger Schutz als moderne kryptografische Zugangslösungen.

Awareness-Lernpunkt

Ein Ausweis oder Funksender ist nicht automatisch sicher, nur weil er digital ist. Unternehmen sollten ältere RFID-, NFC- und Funksysteme regelmäßig bewerten und gegebenenfalls ersetzen.

Plunder Bug

Ein kleiner Ethernet LAN-Tap, der in eine Netzwerkverbindung eingesetzt werden kann, um Netzwerkverkehr zu analysieren.



Kompakter Ethernet LAN-Tap.

Was ist die Gefahr?

Wer physischen Zugriff auf Netzwerkverkabelung hat, kann unter Umständen Netzwerkverkehr beobachten. Unverschlüsselte Daten wären dabei besonders gefährdet.

Awareness-Lernpunkt

Verschlüsselung sollte nicht nur im Internet, sondern möglichst Ende-zu-Ende eingesetzt werden. Zusätzlich helfen physische Sicherheit, Port-Security und Network Access Control.

LAN Turtle

Ein kleines Linux-System, das optisch wie ein gewöhnlicher USB-Ethernet-Adapter wirken kann. Es wurde für Netzwerkadministration und autorisierte Pentests entwickelt.



Netzwerkgerät im unscheinbaren Adaptergehäuse.

Was ist die Gefahr?

Ein unauffälliges Gerät im Netzwerk kann Informationen sammeln, Netzwerkzugriffe ermöglichen oder als dauerhafter Zugangspunkt missbraucht werden.

Awareness-Lernpunkt

Nicht jedes Gerät, das wie ein Adapter aussieht, ist nur ein Adapter. Inventarisierung, physische Kontrollen, NAC, Port-Security und Netzwerkmonitoring helfen bei der Erkennung unbekannter Geräte.

USB Rubber Ducky

Ein USB-Gerät, das sich gegenüber dem Computer als Tastatur ausgeben und automatisierte Eingaben durchführen kann.



Automatisierte Tastatureingaben via USB.

Was ist die Gefahr?

Betriebssysteme vertrauen Tastaturen traditionell stark. Ein Gerät, das wie eine Tastatur erscheint, kann deshalb innerhalb sehr kurzer Zeit viele Eingaben automatisieren.

Awareness-Lernpunkt

Fremde USB-Geräte sollten nicht einfach angeschlossen werden. Gerätekontrolle, eingeschränkte Benutzerrechte, Endpoint-Schutz und physische Sicherheit reduzieren das Risiko.

Shark Jack

Ein kleines Linux-basiertes Werkzeug für automatisierte Netzwerkaudits.



Mobiles Werkzeug für Netzwerkaudits.

Was ist die Gefahr?

Ein frei zugänglicher Netzwerkanschluss kann einem unbekannten Gerät Zugang zum internen Netzwerk ermöglichen. Schon die Erfassung der vorhandenen Systeme kann wertvolle Informationen liefern.

Awareness-Lernpunkt

Ungenutzte Netzwerkports sollten deaktiviert werden. 802.1X, NAC, Segmentierung und Monitoring erschweren den Zugang unbekannter Geräte.

Pwnagotchi

Ein Raspberry-Pi-basiertes Lernprojekt, das WLAN-Umgebungen analysiert und WPA-Schlüsselmateriel bzw. Handshakes erfassen kann.



WLAN-Lernprojekt mit automatisierter Handshake-Erfassung.

Was ist die Gefahr?

Bei WPA/WPA2 kann aufgezeichnetes Schlüsselmateriel unter bestimmten Bedingungen offline gegen mögliche WLAN-Passwörter geprüft werden. Schwache WLAN-Passwörter sind deshalb problematisch.

Awareness-Lernpunkt

Lange, zufällige WLAN-Passwörter, WPA3 bzw. professionell konfigurierte Enterprise-WLANs erhöhen die Sicherheit erheblich.

O.MG Elite Kabel

Ein USB-Kabel, in dessen Stecker zusätzliche Elektronik integriert wurde. Äußerlich kann es wie ein normales Kabel wirken.

Was ist die Gefahr?

Ein Kabel ist normalerweise ein Gegenstand, dem kaum jemand Aufmerksamkeit schenkt. Genau dieses Vertrauen kann ausgenutzt werden, wenn sich aktive Elektronik im Kabel befindet.

Awareness-Lernpunkt

Keine unbekannten USB-Kabel oder Ladegeräte an sensible Systeme anschließen. Unternehmen können geprüfte Hardware bereitstellen und USB-Gerätekontrollen einsetzen.



Technik versteckt in einem USB-Kabel.

O.MG Adapter

Ähnlich wie beim O.MG Cable ist Pentesting-Technik in einem scheinbar gewöhnlichen USB-Adapter integriert.



Pentesting-Technik in einem USB-Adapter.

Was ist die Gefahr?

USB-Zubehör wird häufig automatisch als vertrauenswürdig betrachtet. Manipulierte Adapter können dieses Vertrauen ausnutzen.

Awareness-Lernpunkt

Zubehör gehört zur IT-Sicherheitskette. Nicht nur Computer, sondern auch Kabel, Adapter, Docks und USB-Geräte sollten aus vertrauenswürdigen Quellen stammen.

WiFi Pineapple Mk7

Eine Plattform für professionelle WLAN-Sicherheitsaudits, Reconnaissance und die Simulation verschiedener WLAN-Angriffsszenarien.



Plattform für WLAN-Sicherheitsaudits.

Was ist die Gefahr?

Endgeräte versuchen teilweise automatisch, bekannte WLANs wiederzufinden. Gleichzeitig vertrauen Nutzer häufig allein einem bekannten Netzwerknamen. Genau diese Annahmen können missbraucht werden.

Awareness-Lernpunkt

WLAN-Sicherheit besteht nicht nur aus einem Passwort. Sichere Authentifizierung, Zertifikatsprüfung, WPA2/WPA3, WLAN-Monitoring und geschulte Nutzer gehören zusammen.

GADGET 12 / 15

Bash Bunny

Eine programmierbare USB-Pentesting-Plattform, die gegenüber einem Rechner unterschiedliche USB-Gerätetypen darstellen kann.



Programmierbare USB-Pentesting-Plattform.

Was ist die Gefahr?

USB ist weit mehr als nur Datenspeicher. Ein Gerät kann sich beispielsweise als Eingabegerät oder Netzwerkschnittstelle präsentieren. Dadurch entstehen unterschiedliche Angriffsmöglichkeiten.

Awareness-Lernpunkt

USB-Sicherheit darf sich nicht darauf beschränken, USB-Sticks zu verbieten. Device Control, eingeschränkte Benutzerrechte und physische Sicherheit sind ebenso wichtig.

GADGET 13 / 15

Packet Squirrel

Ein kleines Ethernet-Pentesting-Gerät, das inline in eine Netzwerkverbindung eingesetzt werden kann.



Kleines Werkzeug zur Ethernet-Analyse.

Was ist die Gefahr?

Befindet sich ein fremdes Gerät physisch zwischen zwei Netzwerkkomponenten, kann es je nach Umgebung Netzwerkverkehr analysieren oder beeinflussen.

Awareness-Lernpunkt

Ende-zu-Ende-Verschlüsselung, Netzwerkzugangskontrolle und physische Kontrolle von Verkabelung und Netzwerkkomponenten sind wichtige Schutzmaßnahmen.

Screen Crab

Ein Gerät, das zwischen HDMI-Quelle und Bildschirm eingesetzt wird und Bildschirminhalte erfassen kann.



Inline-Gerät für HDMI-Bildsignale.

Was ist die Gefahr?

Auf einem Bildschirm können Passwörter, vertrauliche Dokumente, interne Systeme, Kundendaten oder Videokonferenzen sichtbar sein. Ein manipuliertes Zwischenstück kann deshalb erhebliche Informationen erfassen.

Awareness-Lernpunkt

Physische Sicherheit endet nicht am PC. Auch HDMI-Adapter, Dockingstations, KVM-Systeme und andere Zwischenhardware gehören zur Vertrauensketten.

Key Croc

Ein Pentesting-Implantat, das zwischen Tastatur und Computer eingesetzt werden kann und Tastatureingaben erfassen kann.



Hardware-Keylogger und Pentesting-Implantat.

Was ist die Gefahr?

Tastatureingaben können Passwörter, Nachrichten, Kundendaten, Suchbegriffe oder andere sensible Informationen enthalten. Ein unauffälliges Hardware-Implantat kann diese Informationen auf Hardwareebene erfassen.

Awareness-Lernpunkt

Physische Kontrolle von Arbeitsplätzen und USB-Verbindungen ist relevant. Passkeys, Hardware-Token und MFA können außerdem verhindern, dass ein erfasstes Passwort allein für einen Zugriff ausreicht.

ZWISCHENFAZIT

Was bleibt hängen?

Angriffsfläche kennen

Wissen, welche eigenen Systeme aus dem Internet sichtbar sind – und nicht benötigte Dienste abschalten.

Vertrauen hinterfragen

Ein Kabel, ein Adapter, ein WLAN-Name oder eine Tastatur sind nicht automatisch harmlos.

Zugänge härten

MFA, Passkeys, WPA3, Zertifikatsprüfung, Port-Security und NAC erschweren Angriffe erheblich.

Unbekannte Geräte erkennen

Inventarisierung, Netzwerkmonitoring und physische Kontrollen machen Fremdgeräte sichtbar.

Menschen sensibilisieren

OSINT lebt vom Aggregationseffekt – jede veröffentlichte Information ist ein Puzzleteil.

Auf den Ernstfall vorbereiten

Backups, Incident-Response-Prozess und klare Verantwortlichkeiten, bevor etwas passiert.

TEIL 3 · FAZIT

Erhalte die **Kontrolle** zurück

Prävention ist wichtig. Genauso wichtig ist die Vorbereitung darauf, dass Prävention einmal nicht funktioniert. Wie Enginsight dabei hilft.

Enterprise-Security aus Deutschland

Enginsight ist eine Cybersecurity-Plattform, die Angriff und Verteidigung in einem System vereint: automatisierte Risikoanalyse, Cyberabwehr in Echtzeit und Security-Automatisierung – zu 100 % selbst entwickelt, ohne Abhängigkeit von Dritt-Tools.

Datensouveränität ist Programm: Sie entscheiden, ob Enginsight als SaaS gehostet wird oder On-Premises im eigenen Rechenzentrum läuft – mit voller Daten-Kontrolle.



100 % Made in Germany · Innovativ. Effizient. Skalierbar.

 **Gründung 2017**

 **Headquarter in Jena**

 **Über 80 Mitarbeitende**

 **ISO 27001 zertifiziert**

 **Deutscher Support**

 **Mittelstand, Public & KRITIS**

WOFÜR ENGINSIGHT STEHT

IT-Sicherheit einfach gestalten – eine Plattform statt vieler Tools

Transparenz

Jederzeit wissen, wo die eigene IT-Security steht – Sicherheit durch Sichtbarkeit.

Compliance

DSGVO, BSI, NIS2, ISO 27001, TISAX und DORA mit einer Plattform einfacher nachweisen.

Cyberversicherung

Bessere Voraussetzungen durch dokumentierte, kontinuierliche Kontrollen.

Team entlasten

Automatisierungen übernehmen Routine: Patchen, Härten, Alarmieren, Reagieren.

Mehr Kontrolle

Mehr Sicherheit

Mehr Transparenz

Weniger Tools

Weniger Aufwand

Weniger Komplexität

DIE PLATTFORM

Fünf Bausteine, ein Alarmwesen

Watchdog

Agentlos · kostenfrei

Inventarisierung und Monitoring aller Geräte ohne Agent: Drucker, Switches, OT. Deckt Schatten-IT auf – auch bei MAC-Spoofing.

Pulsar

Agents für Server & Clients

CVE- und Patchmanagement, Systeme zur Angriffserkennung (IDS/IPS), FIM, Mikrosegmentierung, Systemhärtung, APT-Scan mit YARA.

Hacktor

Pentest-Flatrate

Über 850 Angriffsvektoren: Information Gathering, Service Discovery, CVE-Scan, Bruteforce. Wiederkehrend statt Momentaufnahme.

Observer

Websecurity

Blick von außen auf Websites und Webanwendungen: Zertifikate, Ports, HTTP-Header, DNS, Bewertung nach BSI-Vorgaben.

SIEM

Detect & Respond

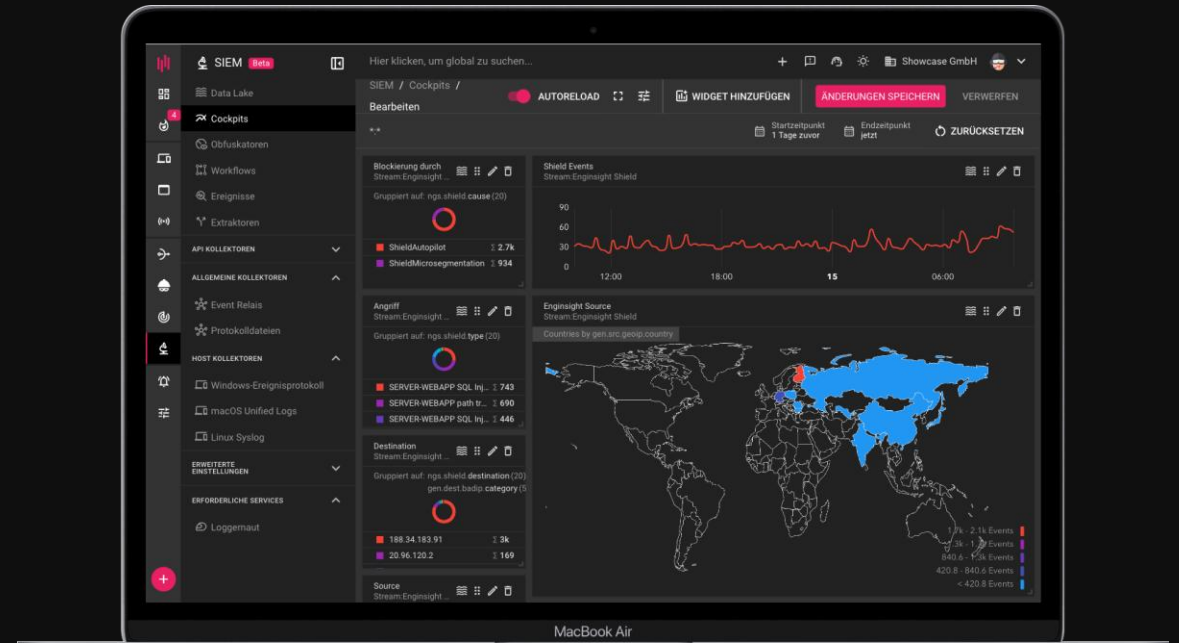
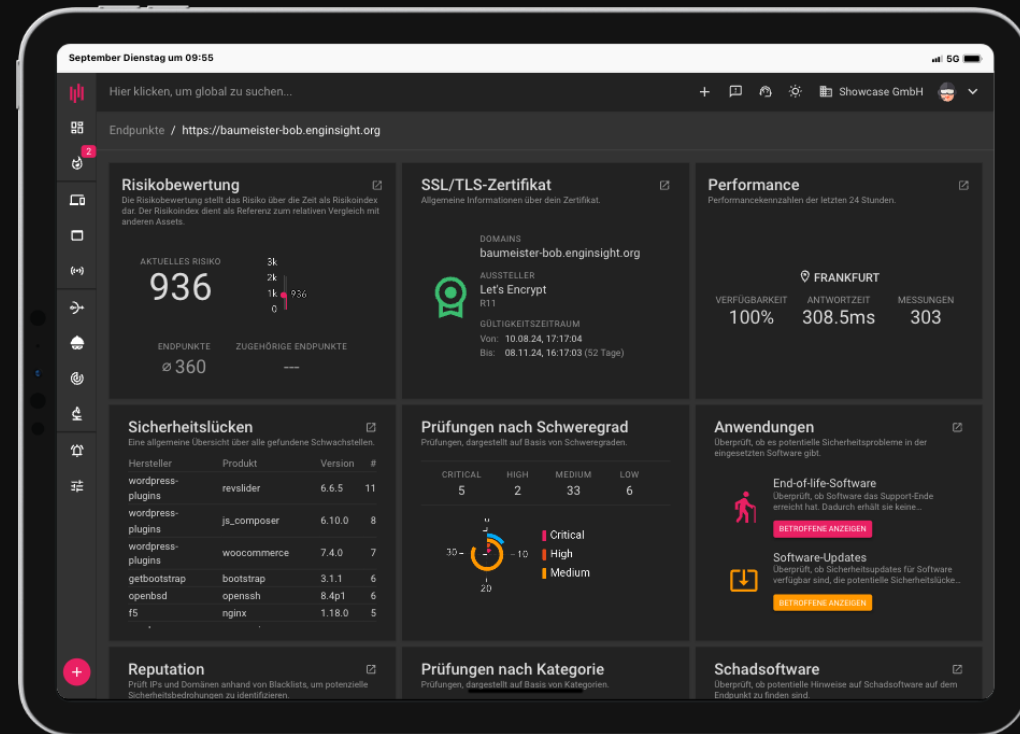
Zentrales Logmanagement, herstellerunabhängig, Log-Flatrate On-Premises, Cockpits, SOAR-Workflows und KI-gestützte Analyse.



Unified Security: ganzheitliche Sicherheit mit einheitlichem Alarmwesen, Anbindung an das Ticketsystem und Dashboards wie CVE-Cockpit, Risikoscores, BSI-Warnmeldungen und Asset Operation Center.

SICHERHEIT DURCH SICHTBARKEIT

So sieht die Kontrolle aus



Wie Enginsight die gezeigten Angriffe erkennt und abwehrt

Szenario aus dem Vortrag	Erkennen	Abwehren
Shodan, Login-Seiten, NAS im Internet – die sichtbare Angriffsfläche	Observer scannt die eigenen Systeme von außen: offene Ports, exponierte Dienste, alte Software	Schwachstellenmanagement mit Risk-Score, Autofix und Patches schließt Lücken, bevor sie gefunden werden
LAN Turtle, Shark Jack, Plunder Bug, Packet Squirrel – Fremdgeräte im Netzwerk	Watchdog meldet jedes neue Gerät mit IP-Adresse; IDS erkennt Port-Scans und ARP-Spoofing	Mikrosegmentierung und automatisches Blocking isolieren verdächtige Geräte; Alarmer starten Workflows
Brute Force auf RDP, SSH oder Web-Logins	IDS/IPS erkennt Anmeldeversuche in Serie – auch im Homeoffice außerhalb der Firewall	Angreifer-IP wird automatisch blockiert; Hacktor testet vorab selbst auf schwache Passwörter

Wie Enginsight die gezeigten Angriffe erkennt und abwehrt

Szenario aus dem Vortrag	Erkennen	Abwehren
Rubber Ducky, Bash Bunny, O.MG Kabel, Key Croc – Angriffe am Endpoint	Pulsar-Agent auf Clients und Servern: Anomalieerkennung, File Integrity Monitoring, Logs im SIEM	SOAR-Playbooks reagieren automatisch; Härtung nach STIGs reduziert Rechte und Angriffsfläche
Ransomware, Erpressung, Notfall	SIEM korreliert Ereignisse über alle Systeme; FIM erkennt Manipulation kritischer Dateien	Incident Response Service und MDR: Experten helfen, wenn Prävention einmal nicht gereicht hat



Technik ersetzt keine Awareness: Backups, MFA, geprüfte Hardware und geschulte Menschen bleiben Pflicht. Enginsight macht sichtbar und automatisiert, was sonst im Alltag untergeht.

WENN PRÄVENTION NICHT REICHT

24x7x365 Managed Detection & Response

Cyber Defence Center in Deutschland

Deutschsprachige Security-Experten überwachen Logs und Events rund um die Uhr, validieren Incidents, leiten aktiv Abwehrmaßnahmen ein und sprechen Handlungsempfehlungen aus.

Erkennung & Abwehr überall

Auf Clients und Servern via Pulsar, in On-Prem-Infrastruktur, Cloud und Netzwerken via SIEM – mit SOAR, Vulnerability Scanning und Network Traffic Analysis.

Inklusive

Proaktives Threat Hunting, Pflege der Detection Rules, Service-Review-Meetings. BSI-qualifizierter APT-Response-Dienstleister und FIRST-Mitglied.

350+

Sicherheits-Expert:innen

2x SOC

24/7 Security Operations Center

400+

Cyber-Defence-Kunden

NIS-2

ISO 27001, TISAX, DORA einfach umsetzen

KUNDENSTIMMEN

Unsichtbares sichtbar gemacht

„Ganz ehrlich: Endlich wissen wir, wo wir stehen. Uns werden die Hosen runtergelassen. Und genau das ist ja das, was wir auch brauchen. Denn wenn wir gar nicht wissen, wo Sicherheitslücken sind, können wir sie auch nicht schließen.“

Sascha Utnehmer, IT-Administrator, Knipping Kunststofftechnik Gessmann GmbH

„Mit Enginsight habe ich eine Ampel, die mir sagt: Vorsicht, da ist was! Und dann kann ich mich drum kümmern. Für mich ist Enginsight deshalb zu einem Leitsystem geworden.“

Mario Haller, Sömmerdaer Energieversorgung GmbH

„Wir waren überrascht, wie einfach und schnell die Einführung mit Enginsight ging. Wir freuen uns, ein so umfassendes Sicherheitsprodukt made in Germany einzusetzen.“

Christian Eckerle, Head of IT, HanseYachts AG

FAZIT

**Sicherheit heißt nicht, alles zu verstecken.
Sicherheit heißt, die eigene Angriffsfläche
zu kennen.**

Awareness für die Menschen. Enginsight für die Technik. Beides zusammen gibt die Kontrolle zurück.



KONTAKT & BOOKING

Vernetzen oder als Speaker buchen?

Persönlicher Austausch

Für Vernetzung, Fragen zu meinen Projekten oder einfach einen lockeren Tech-Talk:
[linkedin.com/in/henry-werner](https://www.linkedin.com/in/henry-werner)

Speaker Booking & Business

Anfragen für Vorträge, Awareness-Schulungen oder berufliche Themen bitte direkt per E-Mail:
henry.werner@enginsight.com

henrywerner.eu · enginsight.com