

OT-SICHERHEIT OHNE BLINDE FLECKEN

In industriellen Umgebungen steht die Verfügbarkeit an oberster Stelle. Dadurch entstehen blinde Flecken, die Angreifer gezielt ausnutzen.

185
TAGE

verweilen Angreifer
im Schnitt in OT,
bevor sie Schaden
anrichten

DIE BEDROHUNG KANN BEREITS IM NETZWERK SEIN

OT- und SCADA-Umgebungen sind auf maximale Verfügbarkeit ausgelegt. Viele klassische Sicherheitsmaßnahmen lassen sich dort deshalb nur eingeschränkt einsetzen, ohne den laufenden Betrieb zu beeinträchtigen. Das schafft blinde Flecken, in denen Angreifer lange unentdeckt bleiben können. Häufig werden sie erst sichtbar, wenn bereits Auswirkungen auf den Betrieb entstehen. Das spielt den Angreifern in die Karten: Sie analysieren die Umgebung, identifizieren relevante Systeme und bereiten ihren Angriff sorgfältig vor, bevor sie aktiv werden.

MEHR ALS DATEN STEHEN AUF DEM SPIEL

PROZESSE AUSSERHALB SICHERER GRENZEN

Industriesysteme arbeiten außerhalb sicherer Betriebsparameter.

PRODUKTIONSSTILLSTAND

Jede Stunde Ausfallzeit verursacht messbare Kosten.

SICHERHEITSSYSTEME REAGIEREN NICHT

Systeme zum Schutz von Menschen und Anlagen fallen aus.

In OT-Umgebungen gefährdet ein Angriff nicht nur Daten, sondern auch Prozesse, Produktion und Sicherheit. Die operativen und physischen Folgen reichen weit über das Netzwerk hinaus. Angreifer zielen deshalb nicht nur auf den Zugriff, sondern auf größtmöglichen Schaden.

DAS GESUCHTE ZIEL WIRD ZUR FALLE



OT/SCADA



SENSOR



PLC



HMI

Angreifer suchen in jedem OT-Netzwerk nach bestimmten Zielen. LABYRINTH platziert genau diese Ziele als Decoys (Köder) in der gesamten Umgebung, von der IT-Grenze bis tief in die OT-Segmente, und bildet industrielle Protokolle, Controller, HMIs, SCADA-Interfaces und Engineering-Workstations realistisch nach.

Angreifer stoßen dadurch zuerst auf Decoys, bevor sie operative Systeme erreichen. Der LABYRINTH-Ansatz funktioniert ohne aktive Scans, ohne Beeinträchtigung der Verfügbarkeit und innerhalb der besonderen Rahmenbedingungen industrieller Umgebungen.

Ein konkreter Einsatz zeigt den Effekt: Ein individuell konfigurierter LABYRINTH-Decoy bildete eine SCADA-Schnittstelle in einem operativen Segment nach und erkannte auch Wochen nach der Implementierung wiederholte Zugriffsversuche. Produktionssysteme und Prozesse blieben unberührt, während die Aktivitäten des Angreifers vollständig erfasst wurden.



SERVER/
WORKSTATION



NETWORK
SERVICES



IOT-GERÄTE



WEB
INTERFACES



BREADCRUMBS

DIE VORTEILE IM ÜBERBLICK

✓ ZERO-DAY-ANGRIFFE ERKENNEN

LABYRINTH erkennt gezielte und komplexe Angriffe ohne Signaturen oder Regeln und **ohne vorherige Kenntnis** der Bedrohung. Unbekannte Bedrohungen und Zero-Day-Angriffe werden erkannt, sobald sie aktiv werden. Proprietäre, speziell entwickelte **Decoys** bilden dabei **reale Assets** in **IT- und OT-Umgebungen** realistisch nach.

✓ HANDELN, BEVOR SCHADEN ENTSTEHT

Jede Sekunde, in der ein Angreifer unbemerkt agiert, bringt ihn näher an das, was zählt. LABYRINTH erkennt Bedrohungen **beim ersten Kontakt** und **hält Angreifer** mit Decoys **beschäftigt**. So gewinnt Ihr Security-Team Zeit für die Reaktion, während **echte Assets unangetastet bleiben**.

✓ SCHLUSS MIT DER ALARMFLUT

Jeder LABYRINTH-Alert weist auf eine bestätigte Bedrohung hin und liefert Kontext zu Herkunft, Aktivitäten und eingesetzten Tools des Angreifers.

✓ VOLLE KONTROLLE. MAXIMALE UNABHÄNGIGKEIT.

LABYRINTH wird **vollständig** in der eigenen Umgebung betrieben und unterstützt **Air-Gap**-Szenarien. Die Lösung ist ohne Baseline-Erstellung oder aufwendiges Tuning **direkt einsatzbereit**, **beeinträchtigt bestehende Systeme nicht** und lässt sich **flexibel skalieren**.

NIS-2

DORA

NIST

PCI DSS

✓ INTEGRATION IN BESTEHENDE SECURITY-UMGEBUNGEN

LABYRINTH integriert sich in bestehende Infrastrukturen, Security-Tools und Benachrichtigungs-Workflows. Bestehende Systeme müssen nicht ersetzt oder neu aufgebaut werden.

VMware

Hyper-V

Proxmox

Microsoft Azure

AWS

Bare Metal

IT

OT

SaaS

Cloud

Active Directory

SIEM

EDR

XDR

Firewall

SOAR

Notification

IN EUROPA ENTWICKELT. UNTER REALEN BEDINGUNGEN ERPROBT.

LABYRINTH ist ein 2019 gegründetes Cybersecurity-Unternehmen mit Hauptsitz im polnischen Zabrze. Die Deception-Technologie wurde ursprünglich in der Ukraine entwickelt und unter realen Cyberangriffen erprobt. Heute gilt LABYRINTH als führender europäischer Anbieter für Cyber Deception und Preemptive Cybersecurity.

LABYRINTH trägt das Label „**Cybersecurity Made in Europe**“, ist Mitglied des **CyberMadeInPoland** Clusters und liefert **souveräne europäische Cybersicherheit** an Kunden weltweit. Die vollständig selbst gehostete Lösung verfolgt einen strategischen Ansatz für Preemptive Cybersecurity: Bedrohungen frühzeitig erkennen, bevor sie Schaden verursachen, ohne zusätzliche operative Komplexität für Security Teams.

SICHERHEITSLÜCKEN NACHHALTIG SCHLIEßEN

Machen Sie Ihre OT-Umgebung zum LABYRINTH.

