## Mit Honeypots Angriffe abwehren

# Ein Köder für Cyberkriminelle

**Lösungen zur Angriffserkennung schützen IT- und OT-Netzwerke vor Cyberattacken. In Industrieunternehmen mit komplexen oder älteren Produktionssystemen könnten Honeypots eine bessere Wahl darstellen als klassische Lösungen mit Intrusion Detection-(IDS) und Intrusion Prevention-Systemen (IPS).**

Eine Angriffserkennung, die automatisiert und in Echtzeit über IT-Sicherheitsvorfälle informiert, ist für Unternehmen schon aus reinem Selbstschutz sinnvoll. Für immer mehr Firmen wird dies sogar zur Pflicht. Denn neben KRITIS-Betreibern müssen ab Mai 2023 auch Betriebe, die allein wegen ihrer Größe von besonderem öffentlichem Interesse sind, sowie deren Zulieferer Maßnahmen gegen Hackerangriffe ergreifen. Das schreibt das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) vor. Wie Unternehmen die Vorgabe umsetzen, bleibt ihnen selbst überlassen. Gesetzeskonform sind laut einer kürzlich veröffentlichten Handreichung des BDI zwei Lösungen: IDS/IPS und Honeypots.

### IDS, IPS und Honeypots

Eine Cybersecurity-Strategie, die sich auf die Abwehr von Eindringlingen ins Netzwerk fokussiert, setzt üblicherweise IDS (Intrusion Detection Systems) und IPS (Intrusion Prevention Systems) kombiniert ein. Beide Systeme arbeiten annähernd gleich, indem sie automatisiert auf Abweichungen von zuvor definierten Parametern reagieren. Dabei dient das IDS als Netzüberwachungs- und Benachrichtigungstool. Es löst Alarm aus, sobald es eine Anomalie erkennt. Das Augenmerk richtet sich dabei auf ein breites Spektrum, das von neu angeschlossenen Geräten über Malware-Verhalten bis hin zu unerwarteten SPS-Programmierungen reicht. Das IPS ergreift Gegenmaßnahmen, indem es nicht autorisierte Datenpakete blockiert oder Verbindungen unterbricht. Im besten Fall werden Angreifer so ausgesperrt.

### Mit Honeypots locken

Eine andere Taktik verfolgen Honeypots. Dabei handelt es sich um Köder, die Angreifer gezielt anlocken sollen. Sie imitieren attraktive Angriffsquellen, etwa Server, Steuerungen oder PCs. Als virtuelle Maschinen in die Infrastruktur integriert, sind sie einfach zu finden und weisen bewusst Sicherheitslücken auf, die Hackern vermeintlich Tür und Tor öffnen. Erfahrungsgemäß wählen Angreifer den einfachsten Weg, indem sie Netzwerke scannen und gezielt nach den anfälligsten Geräten suchen, um darüber einzudringen. Da die Honeypots aber keine realen Bestandteile des Netzes sind, leiten sie Kriminelle systematisch in die Irre. Das bindet bei den Hackern Ressourcen und verschafft zugleich den angegriffenen Unternehmen Zeit, um zu reagieren. Die Methode empfiehlt sich vor allem in Fertigungsbereichen mit Legacy Systemen, älteren Maschinen und Anlagen, für deren Software es keine Updates mehr gibt und Patches nicht aufgespielt werden können. Dasselbe gilt für komplexe Systeme, wie SPSen, auf die gängige Sicherheitssysteme nicht zugreifen können bzw. die proprietäre Protokolle nutzen, die für standardisierte IDS/IPS nicht lesbar sind.

### Großflächig einsetzen

Am wirksamsten sind Honeypots, wenn sie großflächig eingesetzt werden und somit eine breite Angriffsfläche bieten.

Bild: ©weyo/stock.adobe.com

IT&Production

**Auszug aus IT&Production, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 07/2022.**

Durch die technische Weiterentwicklung sind sie mittlerweile – auch im Vergleich zu IDS/IPS – kostengünstig und für den Einsatz in der OT einfach konfigurierbar. Auf einer Anwendung lassen sich mehrere zehntausend Honeypots einsetzen. Im Idealfall sollten wichtige Netzsegmente jeweils zur Hälfte aus echten und unechten Systemen bestehen. Cyberangriffe werden normalerweise von langer Hand geplant und innerhalb von Minuten durchgeführt. Honeypots bemerken bereits in einer frühen Phase, wenn jemand unautorisiert im Netzwerk unterwegs ist. Da sie nur bei echten Angreifern, Viren oder Trojanern anschlagen, erzeugen sie wenige, aber dafür qualitativ hochwertige Nachrichten. Anders beim IDS/IPS: Das System schaltet sich erst ein, wenn es Datenanomalien erkennt. Das kann auch Fehlermeldungen bei erwünschten Veränderungen verursachen, etwa, wenn wegen einer Urlaubsvertretung ein Update des Betriebssystems von einem anderen Rechner als üblich erfolgt. Oft verhindert dies, dass Unternehmen Angreifer erkennen.

## Attacken laufen ins Leere

Über Honeypots lässt sich zudem steuern, was Cyberkriminelle in Netzwerken sehen. Sie bieten sich etwa bei einem Port-Scan aktiv an. Die ‘unechten’ Betriebssysteme oder Steuerungen, die auf den virtuellen Instanzen laufen, lassen sich beliebig verändern, um mit den Angreifern zu interagieren und sie so lange wie möglich auf den Honeypots zu halten. Als besonders wirksam erweisen sich die Täuschungen (Deception) bei Ransomeware-Angriffen. Gelingt es einem klassischen IDS/IPS, eine solche Attacke abzuwehren, merkt der Angreifer, das er nicht weiterkommt und sucht nach einem neuen Weg. Verschlüsselt er hingegen einen Honeypot, erstickt das den Angriff im Keim. Die Attacke läuft ins Leere und verursacht keinen Traffic mit dem Hauptnetzwerk, da nicht mit Switches, Routern oder Firewalls kommuniziert wird. Besonders relevant ist das für die OT, denn so wird die produktive Umgebung nicht beeinflusst. Mit sogenannten Honey-Boxen, die eine Vielzahl an Honeypots bündeln, lassen sich – je nach Angriffsart – mehr als 50 verschiedene Systemtypen darstellen.

## Management erforderlich

Im Gegensatz zu einem automatisert ablaufenden IDS/IPS benötigt eine Honeypot-Lösung allerdings ein Management. Das System muss betreut, optimiert und überwacht werden, um bei einem Angriff reagieren zu können. Dies kann entweder durch interne Mitarbeiter oder externe Dienstleister geschehen. Der Mehrwert liegt darin, bösartige Aktivitäten zu verlangsamen. Die Zeit, in der sich ein Hacker mit einem für ihn wertlosen Köder beschäftigt, gilt es zu nutzen, um den Angriff zu entschärfen und möglichst viele Daten über den Ablauf zu sammeln. Mit diesen Informationen kann die Sicherheitsstrategie weiter verbessert werden. Unternehmen mit entsprechende Know-how und Personal decken das inhouse ab. Die Alternative sind externe Managed Services, bei denen auf Cybersecurity spezialisierte Dienstleister ihre Kapazitäten und Erfahrungen einbringen.

## Mehr Sicherheit

Um Angriffe zu erkennen können Unternehmen auf ein IDS/IPS setzen, das aktuelle Momentaufnahmen von zentralen Komponenten liefert. Eine ganzheitliche Überwachung durch Honeypots eignet sich vor allem für Industriebetriebe mit komplexen oder älteren Anlagen. Sie wehren Netzwerkangriffe ab, ohne in den produktiven Bereich einzugreifen. Kombiniert mit einer Next Generation Firewall können Honeypots das Sicherheitsniveau von IT- und OT-Netzwerken deutlich erhöhen. ■

Der Autor Nico Werner ist
Head of Cybersecurity
bei der Telent GmbH.

www.telent.de