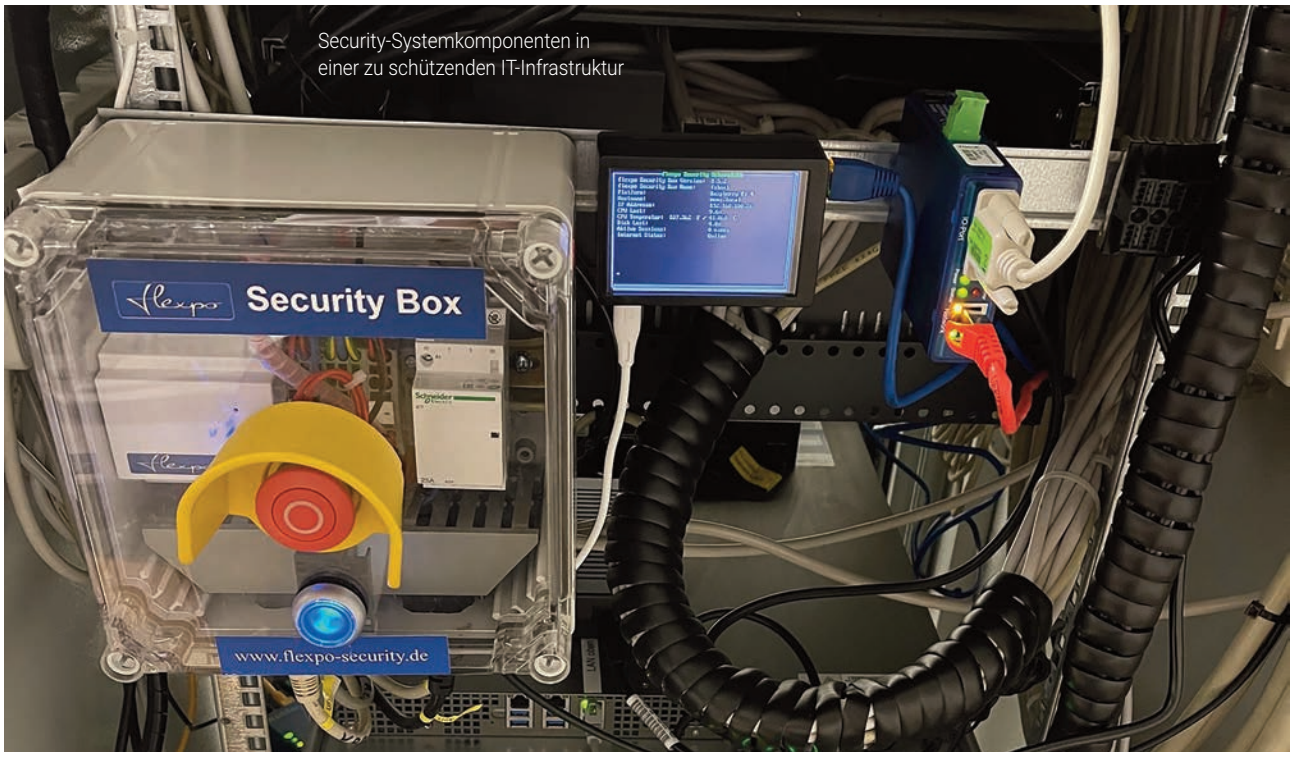
Mit Hardware gegen Cyberangriffe

Systeme abschalten per Kill Switch



Security-Systemkomponenten in einer zu schützenden IT-Infrastruktur

Cyberbedrohungen sind für Unternehmen ein steigendes Risiko. Zwar schützen sich Firmen etwa mit Firewalls gegen Angriffe aus dem Netz. Doch die helfen nicht, wenn eine eingedrungene Ransomware bereits munter interne Daten verschlüsselt. Ein Notschalter – oder Kill Switch – isoliert betroffene Bereiche, um schlimmeres zu verhindern.

In der digitalisierten Welt sind mittelständische Unternehmen mehr denn je auf eine robuste IT-Sicherheitsarchitektur angewiesen. Die Vernetzung von Prozessen und Systemen sowie die wachsende Abhängigkeit von digitalen Technologien erhöhen jedoch das Bedrohungspotenzial. Reaktive Maßnahmen zur Schadensbegrenzung reichen oft nicht mehr aus. Eine Cyber Security Strategie ist unerlässlich. Offensive IT-Sicherheitslösungen, wie das 'Kill Switch Verfahren' ermöglichen hier im Ernstfall eine sofortige Trennung bedrohter Systeme.

Betroffene Systeme isolieren

Cyberangriffe durchlaufen typischerweise verschiedene Phasen. Angefangen bei der strategischen Vorbereitung, in der Angreifer potenzielle Schwachstellen identifizieren, über die Phase der Infiltration, in der sie sich unerkannt Zugang zu Systemen verschaffen, bis hin zum eigentlichen Datendiebstahl und schließlich der Phase der Datenverschlüsselung. Gängige defensive Sicherheitslösungen sind hier oft limitiert. Denn sind die Daten einmal verschlüsselt, ist eine Rückkehr zum Status quo schwierig. Das Kill-Switch-Verfahren isoliert bei Verdacht eines Angriffs Systeme und hindert den Angreifer an der Fortsetzung des Angriffs.

Mehrschichtige Abwehr

Das Verfahren bezeichnet im IT-Kontext eine Notabschaltung, die im Falle eines erkannten Angriffs automatisch und nahezu in Echtzeit eingeleitet werden kann. Betroffene Systeme werden sofort heruntergefahren. Zwar ist ein solcher Not-Aus-Schalter nicht die einzige Methode, um einen Cyberangriff zu

Bild: F&M Consulting Rehage IT-Management

stoppen, aber oft die schnellste und radikalste. Einen solchen Ansatz verfolgt u.a. das System Flexpo IT-Security des Duisburger Systemintegrators F&M Consulting. Diese Lösung setzt auf ein mehrschichtiges Abwehrsystem. Kernstück ist eine Blackbox CPU, die kontinuierlich das Systemverhalten überwacht und nach Anomalien sucht. Erkennt das System eine Bedrohung, etwa durch abweichende Muster (Indicators of Compromise; IoCs), wird die Not-Abschaltung ausgelöst. Diese vor Ort Hardware wird vor und hinter der Firewall der zu überwachenden IT-Infrastruktur installiert und ist für Hacker unsichtbar, da es keine Installation auf Servern oder Netzwerkkomponenten benötigt und für die Kommunikation mit dem Backend in der Cloud, zwei redundante eigene Netzwerke betrieben werden. Ein Messengerdienst der an jedem PC Arbeitsplatz automatisiert installiert und gewartet wird, stellt den Beschäftigten eines Unternehmens ein Frühwarnsystem zu Verfügung. Hier werden etwa über redaktionelle Einträge potentielle und akute Bedrohungslagen gemeldet oder Auffälligkeiten der Sicherheitsagenten sofort an die Arbeitsplätze weitergeleitet. Im Falle eines Cyberangriffs werden auch alle PC Arbeitsplätze über einen Code-red informiert und sofort an ein Notfallscript weitergeleitet.

Mehrere Stufen

Das IT-Scoring sowie die Meldeprozesse laufen über ein Cloud-Backend, das alle Kommunikationskanäle zu den redundaten Netzwerken herstellt. Des Weiteren wird eine Hochverfügbarkeit der Systeme über ein Cluster-Verfahren ermöglicht. Im Falle eines Cyberangriffs mit einer Verschlüsselung wird über ein Scoring Verfahren die Bedrohungsstufe eindeutig als ein Verschlüsselungsmechanismus identifiziert und als Code Red ausgelöst. In einem individuell eingestellten Alarmmanagement erfolgt in mehreren Stufen eine soforige allpolige Abschaltung aller Server und Netzwerke. In Stufe 2 ist es jedoch noch möglich, über eine iOS-Security-App, den Contdown zu stoppen. Wenn dieser nicht in einer definierten Zeit quittiert wird, führt der Vorgang unweigerlich in einen Shutdown der Systeme. Ist auch dieser 'Software Shutdown' bereits durch einen Cyberangriff gestört, so wird ein angeschlossenenes System hart, via Not-Aus Box, abgeschaltet und somit vom Netz getrennt. Die Not-Aus Box schaltet allpolig vor und hinter der USV (unterbrechungsfreie Stromversorgung) die angeschlossenen Systeme stromlos. Eine Batteriepufferung in der Not-Aus Box sorgt dafür, das auch im stromlosen Zustand die Sicherheits- und Zustandsmeldungen an das Security -Backend und die Security App übermittelt werden. Über einen Web-Service, diverser Protokolle und SQL Zugriffe, lassen sich beliebige weitere Sicherheits- und Meldesysteme integrieren. Der bis zu dem Zeitpunkt der automatisierten Abschaltung entstandene Schaden, lässt sich oft bereits mit Schattenkopien der Systeme, im Rahmen einer forensischen Nacharbeit, wieder herstellen.

Anforderungen bewerten

Die Implementierung solcher Mechanismen erfordert eine genaue Bewertung der spezifischen Bedrohungen und Risiken, die für die Organisation relevant sind. Denn oft sind Cyberabwehrmaßnahmen, wie Firewall und Intrusion Detection-Systeme sowie regelmäßige Aktualisierungen der Sicherheitspatches bereits effektive Lösungen und weniger störend für den Geschäftsbetrieb. jedoch Schützen sie nicht bei einem erfolgreichen Übergriff mit vollziehender Verschlüsselung. Das 'Kill Switch Verfahren' reagiert nicht nur passiv auf Bedrohungen, sondern geht aktiv dagegen vor und hilft, potentiellen Schaden zu minimieren. Flexpo IT-Security setzt auf diesen Ansatz und hilft Unternehmen damit beim Schutz gegen Cyberangriffe mit Datendiebstahl und Verschlüsselung. ■

Sascha Gröne
IT-Consultant
F&M Consulting
flexpo-security.de