flexpo IT-Security „Kill Switch“

Digitale Gegenmaßnahme bei Cyberangriffen mit Verschlüsselung

In der heutigen digitalen Ära sind mittelständische Unternehmen mehr denn je auf eine robuste IT-Sicherheitsarchitektur angewiesen. Die zunehmende Vernetzung von Prozessen und Systemen sowie die wachsende Abhängigkeit von digitalen Technologien haben das Bedrohungspotenzial erheblich erhöht. Dabei reicht es nicht mehr aus, lediglich reaktive Maßnahmen zur Schadensbegrenzung zu implementieren. Eine proaktive Cyber Security Strategie ist unerlässlich, um sich gegen hochentwickelte und stetig wechselnde Cyberbedrohungen zu wappnen.

Ein besonderes Augenmerk sollte hierbei auf innovative Verteidigungsmechanismen z.B. den Einsatz von offensiven IT-Sicherheitslösungen, wie das "Kill Switch Verfahren" gelegt werden, welches im Ernstfall eine sofortige Trennung bedrohter Systeme ermöglicht und so weitreichende Schäden verhindert. Dieser Beitrag beleuchtet die dringende Notwendigkeit solcher Strategien und wie mittelständische Unternehmen diese erfolgreich implementieren können.

Warum das „kill Switch Verfahren“ eine wirkungsvolle Methode ist um eine Verschlüsselung der Infrastruktur umgehend zu stoppen.

Cyberangriffe durchlaufen typischerweise verschiedene klar definierte 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 Verschlüsselung, in welcher Daten unzugänglich gemacht oder gar für Lösegeldforderungen gesperrt werden. Hier zeigt sich eine klare Limitation vieler traditioneller, defensiver IT-Sicherheitslösungen: Sind die Daten einmal verschlüsselt, ist eine Rückkehr zum Status quo oft unmöglich. An dieser Stelle offenbart sich die Notwendigkeit proaktiver Ansätze wie dem "Kill Switch“-Verfahren, das bei Verdacht eines Angriffs frühzeitig Systeme isoliert und so den Fortschritt des Angreifers stoppt.

Doch was verbirgt sich hinter dem Kill Switch Verfahren und warum ist es die derzeit effektivste Methode gegen derartige Angriffe?

Das "Kill Switch"-Verfahren bezeichnet im IT-Kontext eine Notabschaltung, die im Falle eines erkannten Angriffs automatisch und nahezu in Echtzeit eingeleitet wird. Es handelt sich um eine offensiv orientierte Technik, die dazu dient, potenziellen Schaden durch einen Cyberangriff drastisch zu minimieren, indem die betroffenen Systeme sofort heruntergefahren werden.

Das "Kill Switch"-Verfahren (Not-Aus-Schalter) ist nicht unbedingt die "einzige" Methode, um einen Cyberangriff zu stoppen, aber es ist oft die schnellste und radikalste Methode, um einen laufenden Angriff zu unterbinden und weiteren Schaden zu verhindern.

Bei einem Kill Switch wird im Wesentlichen die Verbindung oder der Betrieb eines Systems, Netzwerks oder einer Anwendung sofort unterbrochen. Wenn ein Cyberangreifer beispielsweise versucht, Schadsoftware in ein Netzwerk einzuspeisen oder Daten zu stehlen, kann durch die Auslösung des Kill Switches die Verbindung abrupt gekappt werden. Diesen Vorgang möglichst ohne Fehlabschaltungen zu automatisieren bedarf einer besonderen Systemarchitektur.

Eine typische Herausforderung für einen automatisierten Kill Switch.

a.) Eine sehr hohe Systemintegration aller Sicherheitskomponenten
b.) Genaue Kenntnisse von der zu schützenden Infrastruktur und den Geschäftsprozessen.
c.) Agenten und Sensoren die speziell das Verhalten von Massenspeichern analysieren und monitoren, um Datendiebstahl und Verschlüsselungen vom Normalbetrieb unterscheiden zu können.
d.) Ein gut trainiertes System auf den schlimmsten anzunehmenden Fall

auszurichten „der Verschlüsselung“ und „dem Datendiebstahl“

e.) Eine Risikoanalyse der Geschäfts- und Systemprozesse sowie ein individuelles IT-Sicherheitskonzept

f.) Eine Orchestrierung aller IT-Sicherheitssysteme mit einer maximalen Systemdurchdringung.

g.) Eine Kill Switch Lösung benötigt erhebliche Kenntnisse der Geschäftsabläufe und dem Verhalten von Applikationen sowie Systemen und Netzwerken eines Unternehmens und ist nicht auf Signaturen der Angreifer augerichtet, sondern auf Signaturen des zu schützenden Unternehmens. Diese Individualitäten befinden sich alle hinter einer Firewall.

h.) Ein IT-Scoring auf der Ebene von Prozessen, sowie frei programmierbarer Agenten und Aktoren.

i.) Ein Kill Switch kennt genau die Soll Prozesse eines Unternehmens und muss einen einsetzenden Vorgang der Verschlüsselung eindeutig und zweifelsfrei erkennen sowie in sekundenschnelle alle Server hart abschalten.

j.) Der individuelle und administrative Vorgang ist deutlich höher als bei reaktiven IT-Sicherheitslösungen.

In dem folgenden Beispiel wird das Prinzip „Kill Switch“ als Systemlösung „flexpo IT-Security“ erläutert.

Da handelsübliche große wie kleine Monitoring- Lösungen, Cyber Defense , Intrusion Detection, Managed Detection and Response sowie Endpoint Protection Systeme zwar Sensoren einsetzen um Gefahren zu erkennen, jedoch nicht über komplexe freiprogrammierbare Logiken und Scoring Verfahren verfügen, hat sich die Firma F&M Consulting für eine Eigenentwicklung entschieden mit dem Ziel : Eine automatisierte Notabschaltung nach dem Kill Switch Verfahren zu realisieren.

„flexpo IT-Security“- ist eine solche Kill Switch Lösung und setzt auf ein mehrschichtiges Abwehrsystem. Kernstück ist eine **Blackbox CPU**, welche kontinuierlich das Systemverhalten überwacht und nach Anomalien sucht. Erkennt das System eine Bedrohung, etwa durch abweichende Muster „Indicators of Compromise“ (IoCs), wird der „Kill Switch“ ausgelöst und die Systeme umgehend abgeschaltet. 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 (2) redundante eigene Netzwerke betreibt. Ein Messengerdienst (flexpo Service Tool) der an jedem PC Arbeitsplatz automatisiert installiert und gewartet wird, stellt den Mitarbeitern eines Unternehmens ein Frühwarnsystem zu Verfügung.

1.) Über redaktionelle Einträge werden potentielle und akute Bedrohungslagen gemeldet

2.) Auffälligkeiten der Sicherheitsagenten werden sofort auch an die Arbeitsplätze weitergeleitet.

3.) Im Falle eines Cyberangriffs werden auch alle PC Arbeitsplätze über einen Code-red informiert und sofort an ein Notfallskript weitergeleitet.

4.) Nur durch eine zeitnahe Quittierung dieser Meldung, ausgewählter Mitarbeiter, lässt sich ein Countdown noch stoppen.

5.) Aus den IT-Wartungsprotokollen sowie den geplanten und ungeplanten Downtime der Systeme werden die Hochverfügbarkeiten einzelner Systeme berechnet und dienen als ein Cockpit für den IT - Sicherheitsstand in den zu schützenden Unternehmen. Im Falle eines Cyberangriffs mit möglichen Schadensfällen lassen sich auch für Cyberversicherungen eindeutige Nachweise aus diesem Service Tool generieren.

6.) Über ein Microsoft Reporting Services wird eine Dashboard mit allen IT-Sicherheitsmerkmalen generiert, um weitere Lücken oder Prozessveränderungen aufzuzeigen.

Eine zentrale IT-Sicherheitslösung steuert alle Teillösungen

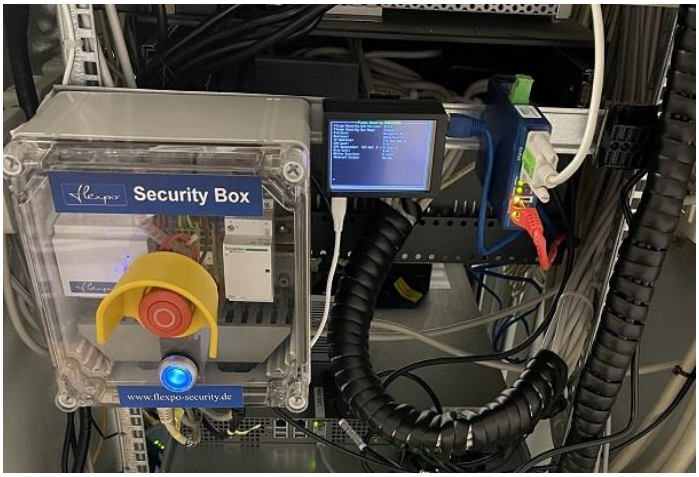


Bild 1 (Systemkomponenten der flexpo -Security in einer zu schützenden IT-Infrastruktur)

Ein Backend in der Cloud übernimmt das **IT-Scoring** sowie die **Meldeprozesse** und stellt alle Kommunikationskanäle zu den redundanten Netzwerken her. Des Weiteren wird eine Hochverfügbarkeit der Systeme über ein **Cluster Verfahren** sichergestellt. 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 und ebenfalls **integrierten Alarmmanagement** erfolgt in Stufen 3 eine sofortige allpolige Abschaltung aller Server und Netzwerk. In Stufe 2 jedoch ist es möglich, über eine **iOS Security-App**, den Contdown zu stoppen. Wenn dieser nicht in einer definierten Zeit quittiert wird, führt dieser Vorgang unweigerlich in einen Shutdown der Systeme. Ist auch dieser „Software Shutdown" bereits durch einen Cyberangriff gestört, so werden diese angeschlossenen System hart, via **Not-Aus Box** abgeschaltet und somit vom Netz getrennt. Die Not-Aus Box schaltet allpolig vor und hinter der USV die angeschlossenen Systeme stromlos. Eine Batteriepufferung in der **Not-Aus Box** sorgt dafür, dass 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. Z.B. über ein VDS Protokoll der Gebäudetechnik oder über einen Web-Service wie in dem Beispiel Bild 1 (dort lassen sich auch andere bedrohliche Fälle wie Wassereintritt im Serverraum oder der Ausfall der Klimaanlage) überwachen.

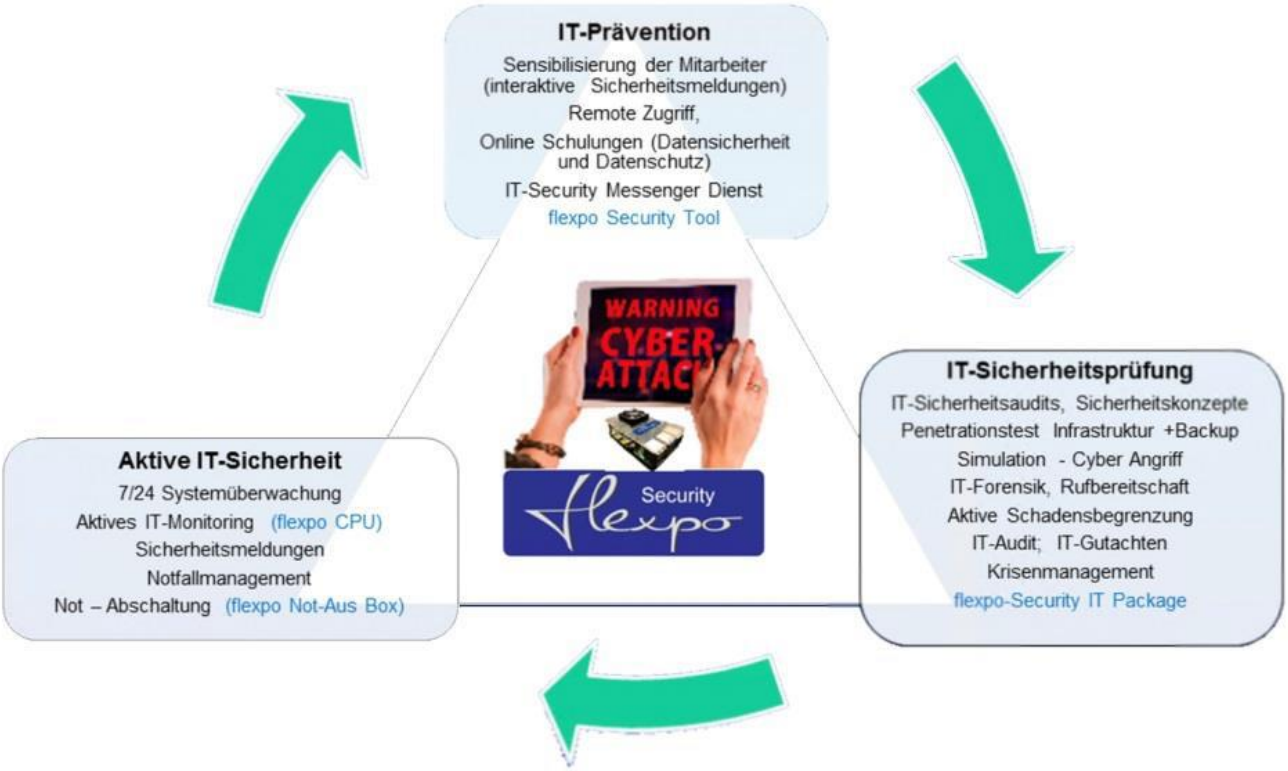


Bild 3 (Zusammenschluss der 3 Sicherheitssäulen im Kampf gegen Cyberangriffe)

Der bis zu dem Zeitpunkt der automatisierten Abschaltung durch einen Kill Switch entstandene Schaden, lässt sich häufig bereits mit Schattenkopien der Systeme, im Rahmen einer forensischen Nacharbeit, wieder herstellen.

Umgang mit Hochverfügbarkeiten von Systemen im Falle einer Verschlüsselung

Bei besonders schützenswerten Geschäfts- und Systemprozessen könnten jedoch auch noch so kleine Betriebsunterbrechung zu hohen Ausfallkosten führen, daher sind auch weitere Ausbaustufen der flexpo IT-Security Suite, als digitaler Service zuschaltbar wie z.B:

a. Redundante Backups (Managed Backup)
b. Redundante Serversysteme (via Cluster Verfahren)

Auch in diesen Serviceabschnitten erfolgt eine automatisierte Umschaltung, im Falle einer Verschlüsselung.

Die Implementierung von IT-Sicherheitsmechanismen wie „Kill Switch“ , erfordert eine genaue Bewertung der spezifischen Bedrohungen und Risiken, die für die Organisation relevant sind. In den meisten Fällen sind konventionelle Cyberabwehrmaßnahmen, wie Firewall und Intrusion Detection-Systeme sowie regelmäßige Aktualisierungen der Sicherheitspatches schon recht effektive und weniger störend für den Geschäftsbetrieb. Schützen aber nicht bei einem erfolgreichen Übergriff mit vollziehender Verschlüsselung.

Der Duisburger Systemintegrator F&M Consulting hat sich daher mit der flexpo IT-Security Lösung gleich für 3 Sicherheitsfundamente einer IT-Sicherheitsstrategie entschieden.

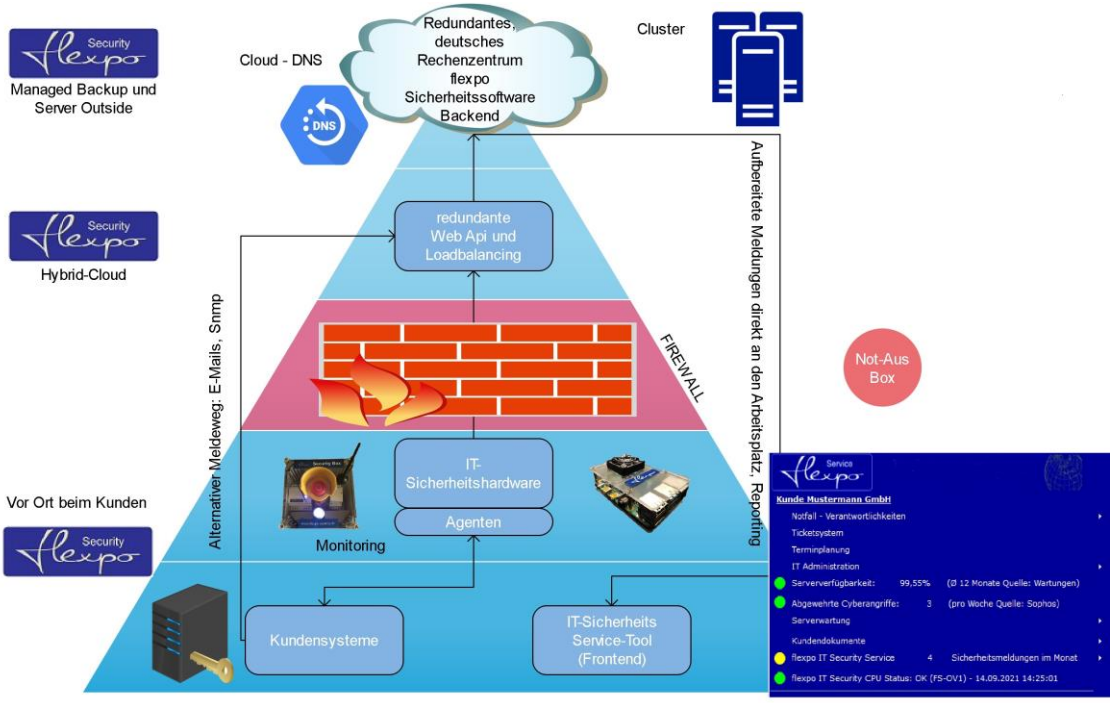
1.) Das flexpo Security Tool als Grundlage für die Prävention „IT-Sicherheit“ Ein Dienstprogramm für jeden Arbeitsplatz um Mitarbeiter zu schulen, trainieren, informieren und zu warnen.
2.) Die IT-Sicherheitsprüfung ,um die Eigensicherheit der Systeme zu testen sowie die Simulation von schädlichen Übergriffen kontinuierlich durchzuführen.
3.) Die aktive IT-Sicherheit als Systemlösung inkl einer sofortigen Not-Abschaltung.

Somit werden sowohl die Maßnahmen der IT-Prävention, kontinuierliche IT-Sicherheitsüberprüfungen und eine aktive Sicherheitslösung bis zum Kill Switch, in einer einzigen Systemintegration unterstützt. Siehe Bild 3

Besonderheiten der flexpo Security Lösung

- Agenten und Sensoren sind für: a.) IT-Systeme b.) Gebäude c.) Prozesse und d.)Hochverfügbarkeit ausgelegt
- Nach einer Risikoanalyse werden Sensoren vor sowie hinter der Firewall installiert.
- **Hinter der Firewall** sind genaue Kenntnisse der zu schützenden IT-Infrastruktur notwendig.
- Für das Trimmen der Sensoren und Aktoren sowie die Erweiterung des IT-Scoring, ist ein kontinuierlicher IT-Security Service nötig.
- Die Hardware läßt sich nicht stoppen und ist nur schwer einnehmbar
- Die **Security CPU** setzt auf ein eigenes Betriebssystem und wird über eine individuelle **Security Disposition** gesteuert.
- Die Anwendungen sowie kundenspezifische Einstellungen sind verschlüsselt abgelegt.

Bild 2 (Technologieschema der zusammenwirkenden IT-Security Komponenten, 1. Security CPU, 2. Not-Aus-Box, 3. Service Tool am Arbeitsplatz)



- Alle Agenten, Sensoren und Aktoren werden sowohl in der **Security CPU** vorgehalten also mit einem Backend in der Cloud repliziert.
- Selbst wenn die Verbindung zum Internet oder Intranet unterbrochen wird, arbeitet die IT-Sicherheitslösungen weiter und kommuniziert über eine Fallback.
- Die Not-Aus Box ist über ein eigenes Netzwerk mit der **Security CPU** verbunden und kann selbst im stromlosen Zustand noch Meldungen an die **flexpo Security App** weiterleiten.
- Die **Not-Aus Box** kann ebenfalls auch manuell über einen NOT-Aus Schalter stromlos geschaltet werden und wird auch in diesem Fall eine Zustandsmeldung noch absetzen können.
- Die versiegelten Hardwarekomponenten werden bei diese IT-Sicherheitslösung von der F&M beigestellt und sind ein fester Bestandteil eines IT-Sicherheits Packages.

Fazit:

Das „Kill Switch“-Verfahren stellt eine revolutionäre Methode im Kampf gegen Cyberangriffe dar. Es reagiert nicht nur passiv auf Bedrohungen, sondern geht aktiv dagegen vor und minimiert so potentiellen Schaden. Die „flexpo IT-Security“ Lösung von F&M Consulting setzt genau auf diesen Ansatz und bietet Unternehmen so einen effektiven und zeitgemäßen Schutz gegen Cyberangriffe mit Datendiebstahl und Verschlüsselung.

Autor

Sascha Gröne

F&M Consulting
IT-Consultant
Organisations- und Technologieberatung
für den Mittelstand

Entwicklungsleiter IT-Security
eMail: support@flexpo-security.de
Internet: flexpo-security.de

Fachinformatiker Anwendungsentwicklung , EDV Sachverständiger und Gutachter , Zertifizierter EU – Datenschutzbeauftragter

Weitere Kernkompetenzen sind:

flexpo-Industrie
flexpo-Systemlösungen
IT-Outsourcing