Cyber-Kriminalität seit Jahren auf dem Vormarsch

Wer sind die Opfer?

Kurz gesagt: Jeder kann Cyber-Attacken zum Opfer fallen. Die Presse berichtet beinahe täglich über Angriffe mit Ransomware auf die verschiedensten Ziele. Hacker suchen sich nur selten gezielt Organisationen als Ziele aus; meist dringen sie dort ein, wo sich die Chance dazu bietet. **Unternehmen aus allen Branchen werden genau so Opfer von Erpressungs-Trojanern wie Krankenhäuser, Schulen und Universitäten, Stadtverwaltungen und öffentliche Einrichtungen.** Bei weitem nicht alle Fälle werden öffentlich bekannt doch allein in den letzten Monaten gab es zahlreiche aufsehenerregende Meldungen:

- Kürzlich wurde ein namhafter taiwanesischer Computerhersteller erpresst, die Hacker forderten 50 Millionen US-Dollar, anderenfalls würden geheime Daten online veröffentlicht.
- Nachdem bei einem japanischen Autohersteller wichtige Systeme verschlüsselt wurden standen an mehreren Standorten auf der ganzen Welt die Bänder still.
- In den USA wurde durch eine Ransomware-Attacke eine extrem wichtige nationale Pipeline lahmgelegt. Tausende Verbraucher drohten von der Versorgung mit Erdöl-Produkten abgeschnitten zu werden, es wurde der regionale Notstand ausgerufen.
- Ein schweizer Fenster-Hersteller musste nach einem Befall mit der Ransomware Ryuk Insolvenz anmelden nachdem die EDV-Systeme an 3 Standorten komplett lahmgelegt waren. 170 Mitarbeiter verloren ihre Jobs infolge der Hacker-Attacke.

Wie hoch sind die Schäden?

Die finanziellen Schäden durch Crypto-Trojaner sind gewaltig: Das FBI errechnete, dass **insgesamt über 144 Millionen US-Dollar „Lösegelder" an Hacker gezahlt** wurden – trotz aller Hinweise, dass man im Ernstfall nichts zahlen solle.

Das größte Problem sind allerdings nicht die Lösegelder an sich: Die Cyber-Kriminellen passen die Höhe des Lösegelds inzwischen an Größe und Umsatz ihrer Opfer an, da diese dann eher bereit sind zu zahlen. Weil der Großteil der Betroffenen kleine und mittelständische Unternehmen sind, ist der für die Entschlüsselung der Daten geförderte Betrag meist verhältnismäßig gering – die **finanziellen Auswirkungen können allerdings trotzdem für ein Unternehmen existenzbedrohend sein.**

Eine Untersuchung von 2019 ergab, dass die durchschnittliche Lösegeld-Forderung „nur" 5900$ betrug. **Der Schaden, der durch den Ausfall der EDV entstand, war allerdings im Schnitt 23mal so hoch – also über 130.000$.**

Unsere Lösung heißt FIT!

Das innovative Frühwarnsystem für Ihre IT hilft, Bedrohungen durch Cyber-Attacken frühzeitig zu erkennen und so schneller bekämpfen zu können!
Mehr Infos unter www.f-it.tech

SURITEC

Wir machen Ihr Netzwerk FIT gegen Cyber-Attacken!

www.f-it.tech

FIT: Das einzigartige IT-Frühwarnsystem

Das Problem

Täglich gibt es über das Internet Millionen von Angriffen durch Viren, Trojaner, Malware und anderer Schadsoftware. **Die größte Gefahr geht derzeit von Ransomware aus** – also Trojanern, die darauf ausgelegt sind, die infizierten **Systeme zu verschlüsseln und somit unbrauchbar zu machen bis ein „Lösegeld" bezahlt wird.** Allerdings werden inzwischen auch zunehmend sensible, interne Daten gestohlen und gedroht, diese zu Veröffentlichen wenn das Opfer nicht zahlt. Nicht nur die Veröffentlichung stellt eine Gefahr dar – denn wenn personenbezogene Daten gestohlen werden ist dies ein gravierender datenschutzrechtlicher Verstoß, der zusätzlich noch empfindliche Bußgelder nach sich zieht. Namen wie Emotet, Ryuk und WannaCry sorgten so in den vergangenen Monaten für Angst und Schrecken im Internet.

Unsere Lösung: FIT

FIT ist das **F**rühwarnsystem für Ihre **IT**. FIT beobachtet den Netzwerk-Traffic und löst bei der Erkennung von verdächtigen Anfragen sofort Alarm aus. Dadurch, dass FIT **nicht nur die Art der Bedrohung, sondern auch deren Ursprung** protokolliert, kann Schadsoftware schnell lokalisiert und eingegrenzt werden – im Idealfall kann die Gefahr gebannt werden bevor Daten verschlüsselt oder gestohlen werden oder Sie das gesamte Netzwerk offline nehmen müssen.

FIT vor Ort

Sie haben weitere Fragen zum System von FIT? Sie möchten das Frühwarnsystem für Ihre IT kostenlos und unverbindlich live erleben?

Mit FIT haben Sie den doppelten Vorteil: Sie haben Ihren **persönlichen Ansprechpartner immer vor Ort in der Nähe** und zusätzlich profitieren Sie von unserer **Experten-Hotline, die auf Wunsch rund um die Uhr für Sie erreichbar ist** und Ihnen im Fall eines Angriffs schnell und umfassend berät!

Rufen Sie uns an oder schreiben Sie uns:
Wir beraten Sie gerne individuell!

So schützt FIT Ihre IT in 4 Schritten:

1. Ihr Frühwarnsystem wird vorkonfiguriert geliefert und integriert sich völlig unauffällig in Ihre IT-Infrastruktur. Sie brauchen nichts weiter zu tun als FIT an Ihr Netzwerk anzuschließen.
2. FIT ist sofort einsatzbereit und überwacht Ihr Netzwerk auf verdächtige Anfragen. Dadurch können auch gefährliche Aktivitäten erkannt werden, die Firewalls und Antiviren-Software bereits überlisten konnten.
3. Die einzigartige Software von FIT ist darauf ausgelegt, auffällige Netzwerkaktivitäten sehr schnell zu erkennen und zu melden. Jede Erkennung löst eine Warnmeldung aus, die von unserem Experten-Team geprüft und analysiert wird.
4. Unser Experten-Team informiert Sie umgehend über die erkannte Gefahr. Außerdem erhalten Sie direkt Ratschläge, welche Schritte Sie einleiten sollten um Ihre Daten und Systeme zu schützen.

Ihr Suritec-Experte vor Ort:

www.f-it.tech