Interview: Mit Sascha Gröne

F&M Consulting und flexpo Security

Notabschaltung bei Cyberangriffen mit Verschlüsselung

F&M Consulting , hoch innovative IT-Security Lösung mit NOT Abschaltung

Besonderheit: Duisburger IT Spezialist für Automation und Cybersecurity stoppt Cyberangriffe auf Unternehmens IT.

Herr Gröne, womit ist diese technische Innovation in dem Bereich IT-Security zu begründen ?

flexpo IT-Security ist eine IT Sicherheitslösung mit der Cyberangriffe in kürzester Zeit aktiv gestoppt werden. Dabei wird ein digitaler Gegenangriff gestartet indem eine kontrollierte und automatisierte Abschaltung der zentralen Systeme erfolgt. flexpo IT-Security ist eine umfassende Monitoring- und IT Security Management Lösung, welche bis zur Stromabschaltung bei vollziehenden Cyberangriffen hochautomatisiert eingreift. Durch kontinuierliche Datenanalysen und KI-Scoring mittels Sicherheitshardware und -software vor Ort, aber auch zusätzlich redundanter Systemlösungen in zwei Rechenzentren, werden Abweichungen vom normalen IT Betrieb innerhalb weniger Sekunden erkannt und je nach Bedrohungslage automatisiert gemeldet oder zur sofortigen Abschaltung geführt. Um einen echten Schaden zu vermeiden ist der größte Feind die Zeit, welche zwischen dem Start einer Verschlüsselung und dem andauernden Prozess der Verschlüsselung vergeht. Es bleiben max. 10-20 Minuten für eine totale Abschaltung egal zur welcher Uhrzeit und Wochentag, um im besten Falle nur einen Kollateralschaden zu erleiden.

Interview: Mit Sascha Gröne

F&M Consulting und flexpo Security

Notabschaltung bei Cyberangriffen mit Verschlüsselung

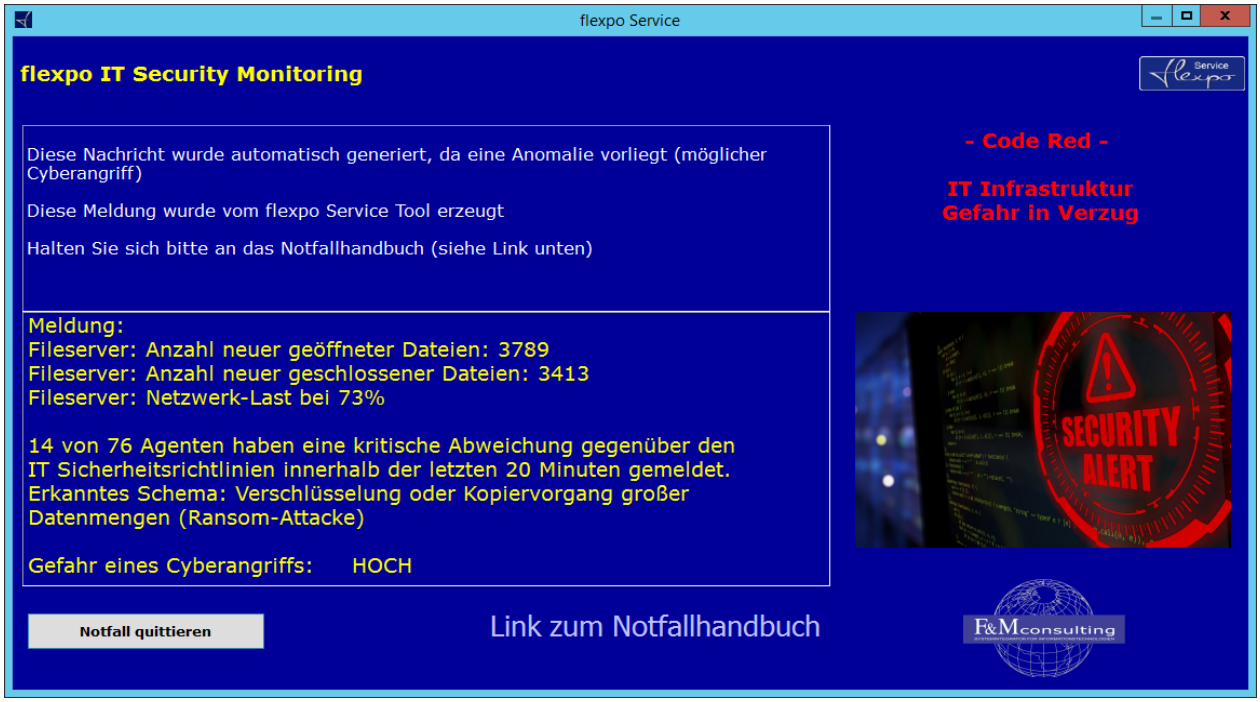
F&M Consulting , hoch innovative IT-Security Lösung mit NOT Abschaltung

flexpo IT-Security konzentriert sich hauptsächlich auf genau diese Schadensreduktion und nicht auf das Unausweichliche. Einen Cyberangriff an sich. Denn dieser wird früher oder später stattfinden.

Dabei wird eine kleine Blackbox CPU für das Monitoring vor und hinter der Firewall der zu überwachenden Unternehmens IT eingesetzt , welches im Sekundentakt Prozessanomalien und Muster nach üblichen Angriffstaktiken (IoCs, Indicators of Compromise) analysiert und mit einem Backend im Rechenzentrum abgleicht.

Diese IT-Security Lösung verfolgt damit eine Offensivstrategie und Technik der aktiven Gegenwehr und NOT Abschaltung bevor erst ein Schaden entsteht.

Die ausgewählten Komponenten sind nicht auf dem Massenmarkt erhältlich, sondern Eigenentwicklungen und liefern daher auch Angreifern keine Informationen über die angewendeten Mechanismen zur Abwehr von Cyberangriffen.



Herr Gröne, was macht die F&M Consulting bei der Abwehr von Cyberangriffen auf eine Unternehmens IT anders als bereits vorhandene marktübliche IT-Sicherheitsvorrichtungen. ?

Der F&M Consulting, als Spezialisten für IT-Sicherheit und Automation, ist es gelungen mit einer speziellen Kombination aus Hardware, Softwareware und Automation,

Interview: Mit Sascha Gröne

F&M Consulting und flexpo Security

Notabschaltung bei Cyberangriffen mit Verschlüsselung

F&M Consulting , hoch innovative IT-Security Lösung mit NOT Abschaltung

Cyberangriffe auf IT-Systeme durch sofortige Gegenmaßnahmen zu stoppen. Derzeitige Systeme können zwar Angriffe erkennen und melden, jedoch als defensive Security Lösung keine aktiven Gegenmaßnahmen einleiten, wie beispielsweise die Systemlösung flexpo Security.

Somit und nur so werden Schäden durch Verschlüsselungen, Datendiebstahl, Erpressung und Betriebsstillstände verhindert. Vergleichbare offensive Security Lösungen wurden bislang überwiegend bei potentiellen Hochwertzielen wie kritischer Infrastruktur (Kraftwerke, Verkehrstechnik) oder bei militärischen Einrichtungen eingesetzt. Jedoch setzen diese Lösungen profunde Kenntnisse der Geschäfts- und Systemprozesse voraus, die mit keiner Standard Defensivlösung zu realisieren wäre. Die Kenntnisse von Abläufen in dem produzierenden Mittelstand aus 20 Jahren der Prozessberatung, waren daher besonders Hilfreich bei der Entwicklung von flexpo Security. Derartige Lösungen lassen sich auch nicht als Hebelprodukte oder im klassischen Strukturvertrieb vermarken und sind daher weniger für Systemhäuser von Interesse. Da diese Security Lösungen individuell gefertigt und betrieben werden, benötigen diese auch eine permanente Kunden- und Systemnähe.

Der Schutz vor dem äußersten Fall einer Infizierung durch Schade Code, ist bei einer offensiven Security Lösung deutlich höher und schränkt auch nicht die Funktionalitäten von Anwendersoftware ein. So, dass das tägliche Arbeiten erheblich erschwert und auch die Systemperformance darunter leiden würden. Diese Eigenschaften bringen jedoch defensive Lösungen eher mit sich.

Interview: Mit Sascha Gröne

F&M Consulting und flexpo Security

Notabschaltung bei Cyberangriffen mit Verschlüsselung

F&M Consulting , hoch innovative IT-Security Lösung mit NOT Abschaltung

Herr Gröne, warum sind Sie diesen Weg gegangen und warten quasi auf den schädlichen Übergriff auf die Unternehmen IT ?

Die Abwehr eines Cyberangriffs ist bei dieser flexpo IT-Sicherheitslösung in mehrere Angriffsstufen gestaffelt und wirkt bereits schon sehr viel früher. Nur diese Maßnahmen können, wie auch alle anderen marktüblichen derzeitigen IT-Sicherheitssysteme, nicht zu 100% einen Übergriff und somit eine Infektion der IT-System verhindern. Lediglich können diese sehr viele Angriffe, wenn überhaupt erkennen, melden, jedoch nicht aktiv und automatisch eingreifen. Ist ein Angriff jedoch in einer Zeit in der keine IT-Personal den Vorfall oder auch einen Alarm bemerkt , so werden alle IT-Komponenten verschlüsselt und meist zuvor auch kopiert.

Bei der flexpo IT-Security Lösung jedoch übernimmt eine zweite wichtige Phase „das Modul NOT-Aus“ einen sofortigen und hoch automatisierten Gegenangriff .

Herr Gröne, wie wirkungsvoll ist dieser Gegenangriff und wie funktioniert dieser in der Praxis ?

Die Wirkung der Erkennung einer Verschlüsselung liegt bei nahezu 100% . Das liegt weniger an dem Verhalten der Angreifer sondern eher an dem Verhalten der angegriffenen Systeme. Hier besitzt die Security Lösung einen Heimvorteil, da das Systemverhalten im Falle einer Verschlüsselung oder Datendiebstahl trainiert wurde. Mit dem Beginn der Verschlüsselung greifen die automatisierten Mechanismen in Sekunden schnelle. Da die Systeme alle sehr spezielle Verhaltensmuster zeigen, welche nicht mehr im Verborgenen bleiben können, ist dieser Ansatz sehr sicher, benötigt aber eine sofortige Handlungsmaßnahme. Da diese Angriffe fast immer Überraschungsangriffe sind und zu Zeiten der Betriebsruhe stattfinden, würde auch ein noch so ausgefeiltes Alarmmanagement nicht innerhalb weniger Minuten zu einer Systemabschaltung führen. Daher wurde das F&M IT-Sicherheitssystem mit einer unabhängigen und für den Angreifer unsichtbaren CPU ausgestattet. Dieses System verwendet ein IT-Scoring Verfahren mit speziellen Ausführungsmechanismen eines Cyberangriffes und kann auch nicht abgeschaltet werden. Selbst ein Internetausfall oder ein Stromausfall würde das System nicht stoppen können.

Interview: Mit Sascha Gröne

F&M Consulting und flexpo Security

Notabschaltung bei Cyberangriffen mit Verschlüsselung

F&M Consulting , hoch innovative IT-Security Lösung mit NOT Abschaltung

Aber warum kann ein Schaden durch einen Cyberangriff mittels einer F&M IT-Sicherheitslösung ausgeschlossen werden ?

Die häufigsten Angriffe sind zwar Blitzangriffe jedoch in den meisten Fällen sind die Angreifer bereits auf den Zielsystemen (strategische Angriffe) und mit dem Umfeld vertraut. Da dieser Zugriff häufig durch Phishing eMails ausgelöst und somit eine bekannte Identität vorgetäuscht wird, erkennen auch noch so professionelle IT-Sicherheitssysteme diese Ausspähung nicht. Möglicherweise auch nicht das flexpo-IT System. Bis zu diesem Zeitpunkt ist in den meisten Fällen aber auch noch kein messbarer Schaden entstanden. Erst wenn die Angriffswelle startet z.B. in der Nacht, Wochenenden oder an Feiertagen, so reichen je nach Unternehmensgröße ca. 1-2 Stunden der Verwüstung aus und alle Systeme sind nicht mehr einsatzbereit. Auch das Einspielen von Backups ist in vielen Fällen nicht mehr möglich, da meist Infrastrukturen, Backups, Gateways , Datenbanken in einem laufenden Betrieb gestört wurden und der 1:1 Zustand nicht mehr hergestellt werden kann. Daher ist der Ansatz der F&M Lösung, sich auf genau diesen Fall zu konzentrieren. In 2 Jahren forensischer Arbeit wurde von den F&M Informatikern und Ingenieuren daher das Verhalten der infizierten Systeme bei Verschlüsselungen und Datendiebstahl analysiert und in einen Sicherheitsalgorithmus einer Blackbox

verpackt. Diese kommuniziert über eigene getrennte Netzwerke (Firmengeheimnis) mit einer Notabschaltevorrichtung. Auch diese NOT-Aus Box ist eine Eigenentwicklung und auf zahlreiche Sonderfälle eines Cyberangriffs mit Verschlüsselung vorbereitet. Diese NOT-Aus Einrichtung schaltet unmittelbar mit dem Beginn einer Verschlüsselung alle Systeme stromlos und verhindert somit einen größeren Schaden. Einen Wideranlauf der IT-Systeme inkl. Beseitigung der Schadsoftware und Änderung aller Passwörter für Systemzugriffe, ist in 3-4 Stunden wieder hergestellt. Im Gegensatz zu einer erfolgreichen Verschlüsselung entsteht bei dieser aktiven Gegenwehr, kein Datendiebstahl, keine Erpressung und kein Betriebsstillstand auf unbestimmt Zeit. Ebenso wird kein Reputationsverlust bei Kunden oder Lieferanten zu beklagen sein.

Bei wie vielen Kunden ist das IT-Sicherheitssystem im Einsatz und hat sich dieses bereits bewährt ?

Das System wird in den verschiedenen Ausbaustufen bereits seit 4 Jahren bei Kunden aus Industrie und Handwerk eingesetzt. Die Möglichkeit einer sofortigen Notabschaltung ist seit 2 Jahren möglich und ebenfalls im Dauereinsatz 7/24.

Zu den Kunden zählen namhafte Automobilzuliefererbetriebe, Nahrungsmittelhersteller, Dienstleistungsbranche, Handwerksbetriebe und aus der Elektronik Branche.

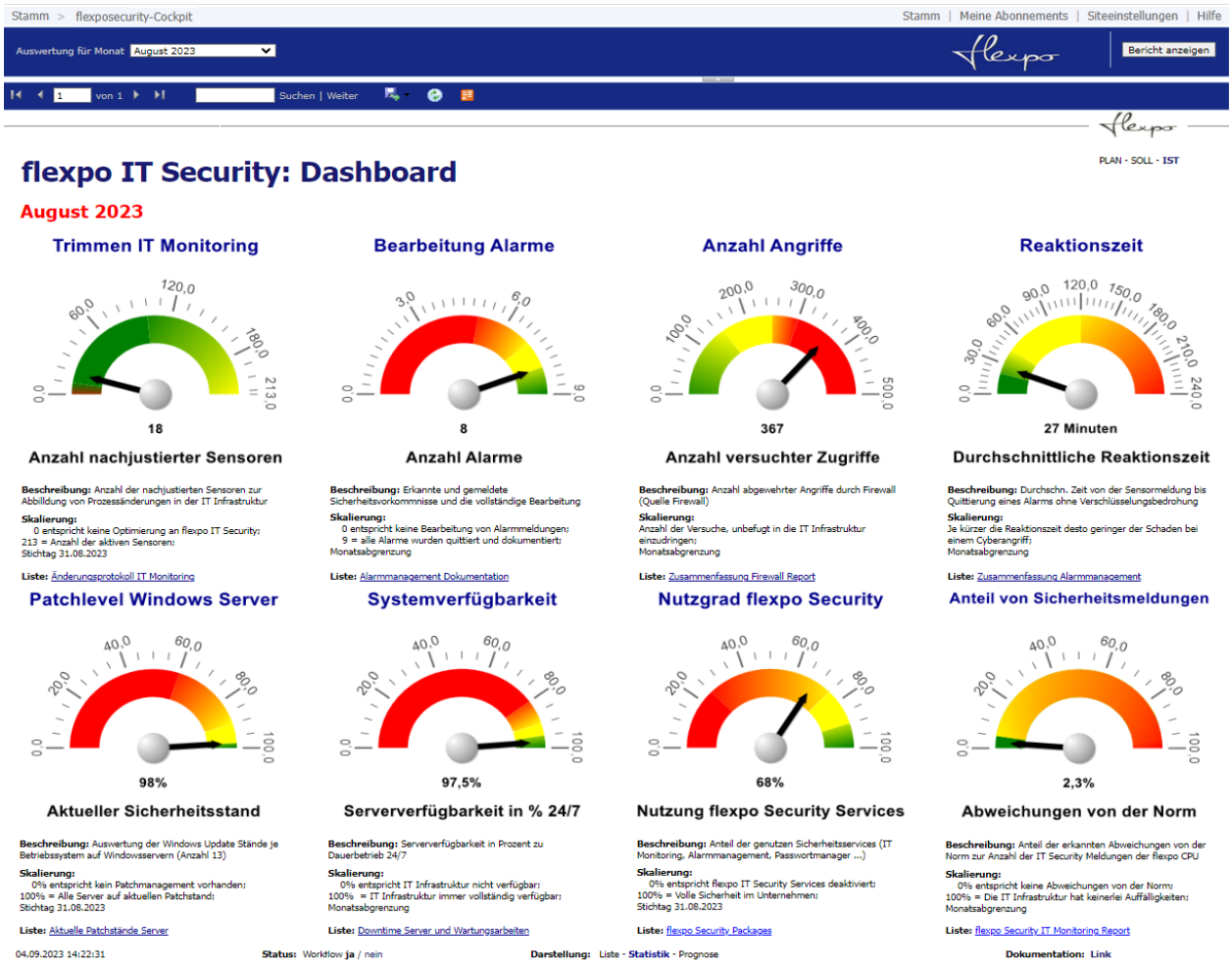
Referenzen können besichtigt und interviewt werden. Dürfen jedoch aus Gründen der IT-Sicherheit nicht der Veröffentlichung dienlich sein.

Interview: Mit Sascha Gröne

F&M Consulting und flexpo Security

Notabschaltung bei Cyberangriffen mit Verschlüsselung

F&M Consulting , hoch innovative IT-Security Lösung mit NOT Abschaltung



Seit dem Einsatz der flexpo IT-Sicherheitslösung gab es bei keinem der F&M Kunden eine Verschlüsselung oder auch Datendiebstahl. Auch die Hochverfügbarkeit der IT-Systeme, ist durch ein ebenfalls von der F&M Consulting entwickeltes Clusterverfahren, auf über 98% angestiegen.

Interview: Mit Sascha Gröne

F&M Consulting und flexpo Security

Notabschaltung bei Cyberangriffen mit Verschlüsselung

F&M Consulting , hoch innovative IT-Security Lösung mit NOT Abschaltung

Was bietet die F&M Consulting den Kunden genau an und ist diese IT-Sicherheitslösung auch für kleine Kunden mit weniger Arbeitsplätzen, aber brisanten Unternehmensdaten gedacht ?

Die IT-Sicherheitslösung wird in Sicherheitspaketen je nach Unternehmensgröße angepasst und ist daher auch für sehr kleine Unternehmen ausgelegt.
Die Sicherheitshardware wird gestellt und bleibt Eigentum der F&M Consulting. Lediglich eine feste Monatspauschale je Unternehmensgröße und ein Sicherheitskontingent für das Trimmen von Sicherheitssensoren, bei veränderter IT-Umgebung, fällt bei dieser Lösung an.
Das System wird einmalig (feste Tagespauschale) vor Ort in Betrieb genommen. Ebenfalls folgen alle Einstellungen einer System Ist-Aufnahme für die Sicherheitstemplates (aller Agenten) und einer Risikoanalyse, auf der Ebene der wichtigsten Geschäfts- und Systemprozesse. Danach wird das Sicherheitslevel und die Sicherheitspakete definiert und scharf geschaltet.

Zur Person: **Sascha Gröne**

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

eMail: support@flexpo-security.de
Internet: www.flexpo-security.de

Fachinformatiker Anwendungsentwicklung
EDV Sachverständiger und Gutachter
Zertifizierter EU – Datenschutzbeauftragter
durch die Deutsche Sachverständigen Gesellschaft (DESAG)

WDR Lokalzeit 1/2023