flexpo IT-Security Service

Der digitale IT Security Service für maximalen Schutz

Der Rundum IT-Sicherheitsschutz für die gesamte Unternehmens IT. flexpo-security.de Dieser engmaschige IT-Sicherheitsservice der F&M Consulting ist derzeit einer der wenigen IT-Sicherheitslösungen welche alle Sicherheitslevel in einer Security Lösung vereint. Durch einen kontinuierlichen Prozess bestehend aus Sicherheitskonzepten, Prüfung der Sicherheitsstufen (Mensch, Systeme, Delinquent), Meldungen potentieller und akuter Bedrohungslagen sowie einen aktiven Eingriff zum Schutz der Unternehms IT, wird dieses hohe Sicherheitslevel erreicht.

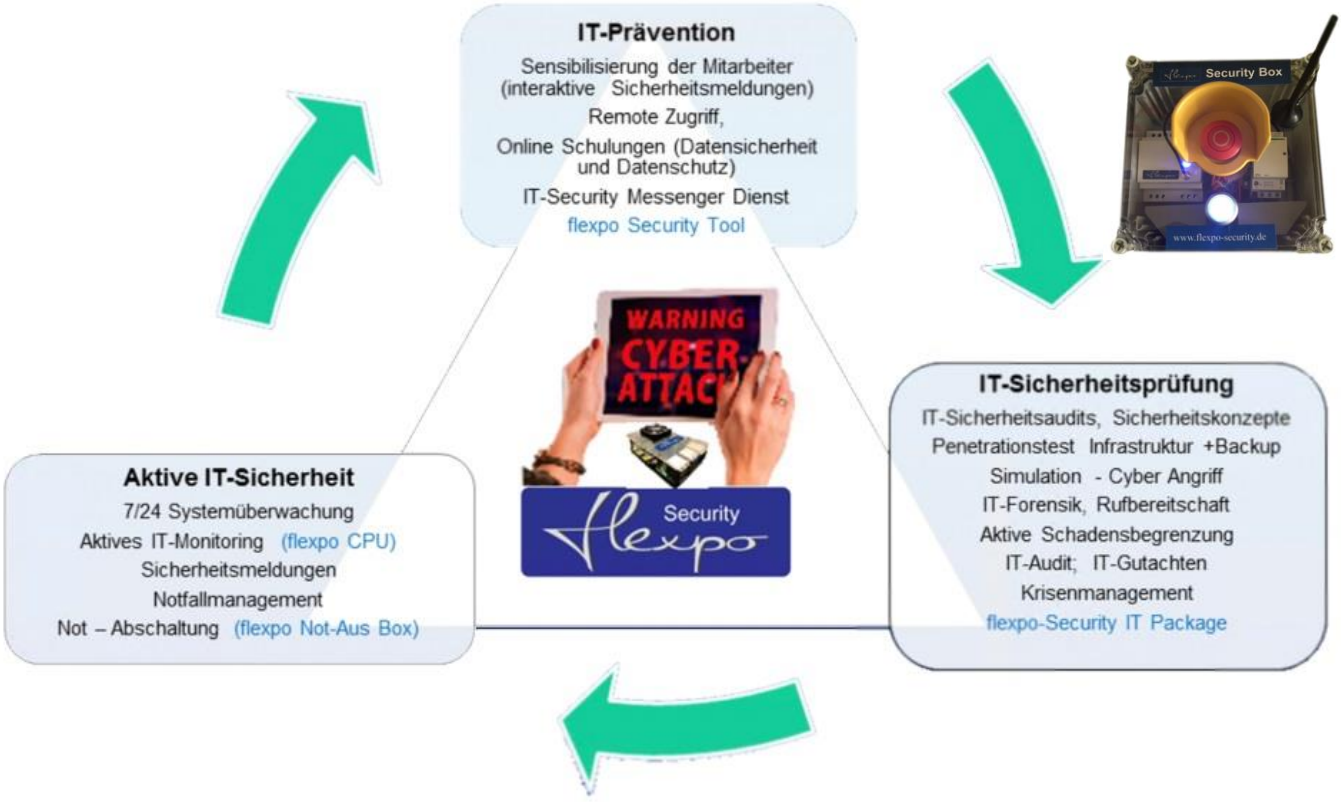
Das 3 Säulen Rundum IT Security Paket

Schützen Sie Ihr geistiges Eigentum und Ihre Unternehmens IT durch den IT-Security Full Service **flexpo Security**
Denn Datensicherheit und Datenschutz (DSGVO) sind die Sicherheitspfeiler für Systeme, Mitarbeiter und dem Unternehmen und schützen vor Erpressung, Sanktionen, Diebstahl geistigen Eigentums sowie Reputationsverlust.

Die F&M Consulting ist Ihr Partner für IT-Sicherheit in Ihrem Unternehmen.

Die Sicherheitsbedrohung

Die häufigste und zugleich perfide Bedrohung für eine Unternehmens IT ist weiterhin und zunehmend die Schadsoftware „Ransomware“. Bereits jedes zweite Unternehmen in Deutschland wurde schon von Schadsoftware infiziert. Der jährliche Schaden durch Schadsoftware kostet die deutsche Wirtschaft 55 Mrd €. Die Ausfallkosten im Zusammenhang mit Ransomware sind im Schnitt 50-mal so hoch wie das geforderte Lösegeld. Der aktuelle Schutz gegen Cyberangriffe ist in 80% aller Unternehmen weit unter dem Mindestmaß, so dass selbst die Höhe der Lösegeldforderungen, die tatsächlichen Kosten der Ausfallzeiten, bei weiten unterschreiten. Dabei sind die Kosten der Systemwiederherstellung noch nicht berücksichtigt. Schließlich können die Angreifer den angerichteten Schaden genau beziffern und kennen durch die meist wochenlange Spionage auch die Kaufkraft der geschädigten Unternehmen. Hinzu kommt häufig der Trugschluss, dass das Einspie-



len einer Datensicherung den Schaden wieder beheben würde.

Was kosten IT-Sicherheit für ein Unternehmen ?

Sicher ist jedenfalls, dass alle gemeldeten oder bekannten IT-Sicherheitsvorfälle mehr kosteten als notwendige Maßnahmen zur Verhinderung dieser gekostet hätten. Zumal die notwendigen IT Sicherheitsmaßnahmen für jedes Unternehmen sehr individuell sind. Erst durch ein IT-Sicherheitsaudit und Sicherheitskonzepte, werden die Sicherheitslücken und somit die notwendigen Maßnahmen zur stetigen Überwachung, Erkennung und Meldung deutlich.

Wie wirksam sind heutige IT-Sicherheitssysteme gegen Cyberangriffe?

Die meisten IT-Sicherheitssysteme beginnen am Startpunkt des Geschehens, dem IT-Arbeitsplatz: Jedoch sind alle Antivirensoftwareprodukte nur so gut wie die bekannten Mutation eines Computervirus, die als Signatur verfügbar sind. Nur die elektronisch erzeugten Mutationen sind 1.000 fach schneller als es Signaturen nachstellen können.
Auch die Kapselung einzelner Arbeitsplätze ist nicht wirkungsvoll genug, da nicht ein einzelner Arbeitsplatz die begehrte Trophäe ist, sondern die zentrale IT. Daher werden die Arbeitsplätze nur als Einfallstor genutzt. In den meisten Fällen von unvorsichtigen und unwissenden EDV Nutzern mit fehlendem Sicherheitstraining. Auch traditionelle Sicherheitsbarrieren (Firewall), welche primär die zentrale IT und das Firmennetzwerk schützen sollten, sind gegen einen mehrstufigen Cyberangriff wirkungslos.

Welcher Schutz ist der Wirkungsvollste und hält die Auswirkung einer Schadsoftware gering ?

Die Vielzahl heutiger Einzelsysteme bieten keinen ausreichenden Schutz, da diese nicht miteinander kommunizieren und auch nicht oder viel zu langsam in das Geschehen einer möglichen Verschlüsselung eingreifen. Aber genau an dieser Stelle entsteht erst der greifbare Schaden für ein Unternehmen.

Wirkungsvoll ist lediglich die Kombination und die enge Verzahnung der IT-Sicherheitsmaßnahmen bestehend aus:

1.) IT-Prävention
2.) aktiver Schutz über Monitoring und KI Module
3.) IT-Sicherheitsüberprüfung

Besonders wichtig ist der schnelle und aktive Eingriff im Falle einer Ausbreitung von Schadsoftware. Jedoch an dieser Stelle scheitern die meisten IT-Sicherheitslösungen. Denn wer oder was schaltet in der Nacht ein System ab ? Wie wird die weitere Ausbreitung der Schadsoftware aufgehalten ? Und funktioniert überhaupt eine zentrale Abschaltung, wenn der Angreifer das Schloss gewechselt hat (Kein Internet, kein Shuttle) ?

Mit dem **flexpo IT Security Service** bietet die F&M Consulting einen Rundum Schutz für die gesamte Unternehmens IT bis zu aktiven Abschaltung im Falle einer realen Bedrohungslage durch einen Cyberangriff.
IT-Systeme, welche die gesamte Infrastruktur und alle Business Applikationen in Unternehmen ablichten, repräsentieren das Nervensystem eines jeden Unternehmens. Die Digitalisierung und konsequente Vernetzung der Systeme sorgen für effizienterer Abläufe in den Unternehmen und schaffen Hochverfügbarkeit bei weniger Personalabhängigkeit. Prozess und Produkt Know How, sowie Fertigungsüberwachungen und –steuerungen werden bereits durch die digitale Transformation von Business Applikationen übernommen. Der Stillstand eines oder auch mehrerer Systeme z.B. durch einen Cyber Angriff bedeutet für eine Vielzahl von Unternehmen den kompletten Stillstand des Unternehmens. Einen 100% Schutz vor Cyber Angriffen wird es nie geben, da der Jäger dem Gejagten immer einen Schritt voraus sein wird. Wie auch in der Medizin ist ein Schutz nur für eine bestimmte Ausprägung eines Virus entwickelt, nicht jedoch für eine Mutation. 80% aller Unternehmen sind auf Cyberangriffen nicht genügend vorbereitet und rüsten sich mit einem Teilschutz aus Antivirensoftware, Firewall und im besten Fall noch mit Aufklärungsarbeiten bei den IT Usern. Aber der aktuelle Sicherheitsstand der IT wird nicht auf wirksame Gegenmaßnahmen geprüft. Und im schlimmsten anzunehmenden Fall, einer gefährlichen Infektion durch einen Computervirus, sind fast 100% der Unternehmen schutzlos oder greifen viel zu spät in die Ausbreitung der Infektion ein.
Nach zahlreichen Praxisstudien von Cyberangriffen wurde von IT- Sicherheitsexperten der F&M Consulting ein Zeitfenster ermittelt, welches einen kritischen Ausbreitungsgrad von Schadsoftware beschreibt. **So steigen z.B. die verursachten Sach- Vermögens- und Reputationsschäden durch Verschlüsselungen und Datendiebstahl ca. 45 Minuten nach der Infektion exponentiell an**. Nach dieser verstrichenen Zeit dauern

die Wiederherstellungen der IT-Systeme Wochen bis zu mehreren Monaten, um einen 100% Betriebszustand wie vor der Infektion wieder herzustellen. Bei Datendiebstahl gibt es sogar keinen Urzustand mehr. Lediglich eine Lösegeldzahlung kann dann noch weitern Schäden abwenden.

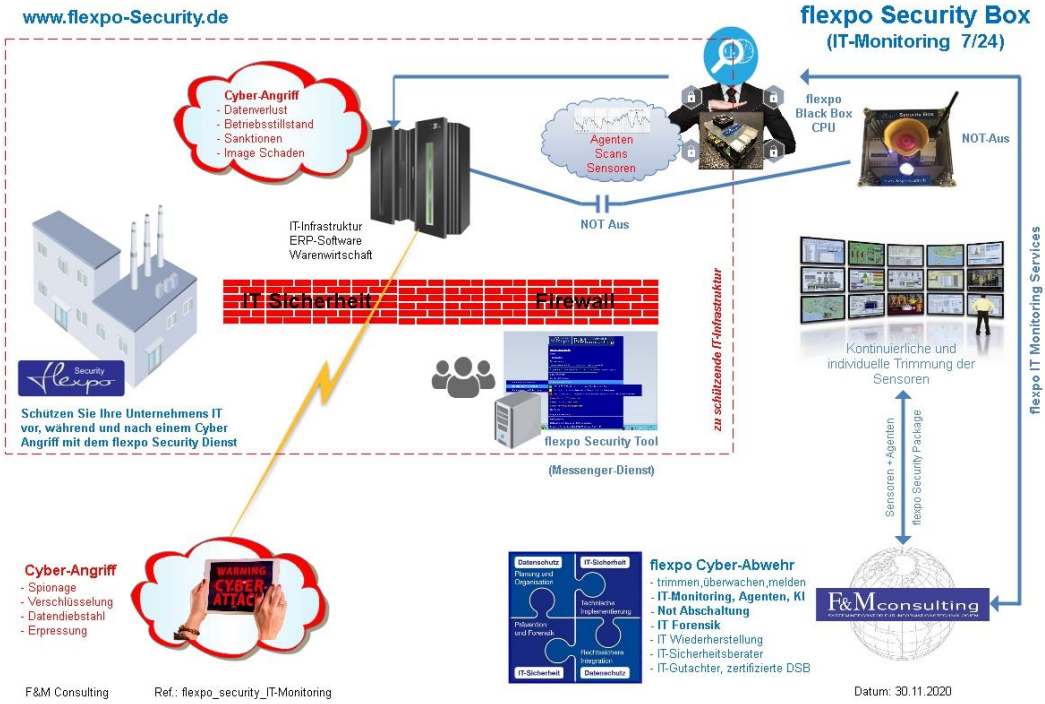
Die F&M Consulting hat sich mit dem IT-Sicherheitskonzept flexpo Security genau auf dieses Zeitfenster konzentriert. Also genau an dieser Stelle, wo kein Sicherheitssystem mehr wirkungsvoll greift, aber die Wahrscheinlichkeit eines Angriffs mit Folgeschäden bei nahezu 100% liegt und es wird nicht bei einem bleiben.

Denn IT-Sicherheitsvorfälle kosten mehr als die Maßnahmen die diese verhindert hätten.

Leider sind das die bitteren Schattenseiten der Digitalisierung. Selbst im Falle einer abgeschlossenen Cyberversicherung können bestenfalls einige Vermögensschäden aufgefangen werden und auch nur, wenn das Unternehmen die lückenlose IT-Sicherheitsmaßnahmen, wie vertraglich zugesichert, nachweisen kann. Der Betriebsstillstand, die Unsicherheit und der Reputationsverlust hingegen bleiben.

Verhindern kann man einen Cyberangriff letztendlich nicht aber die Folgeschäden lassen sich kontrollieren.

Der Duisburger IT-Spezialist für Automation und IT-Sicherheit hat ein IT-Sicherheitssystem entwickelt , welches alle Sicherheitsebenen in Unternehmen vor Cyber Angriffen schützt.



Die Besonderheit besteht darin, dass alle Einfallstore einer Schadsoftware in dem einem Sicherheitskonzept, bestehend aus Hardware und Software, gleichermaßen Berücksichtigung finden. Die häufigsten Einfallstore sind dabei:

- Der EDV Benutzer“ Endpoint“ (häufig als Türöffner)

Schutz durch Online Sensibilisierung , Meldung, Training, Übung – Notall

- Die zentrale IT (Firewall)

Schutz durch aktives Auslesen, vergleichen KI, melden

- Die physischen und virtuellen Server -

IT-Monitoring, Agenten und Sensoren, kont. Trimmung

- Alle aktiven IT Komponenten (Gateways, Switche, IOT und weitere Komponenten)

IT-Monitoring, Agenten und Sensoren, kont. trimmen, Pen-Test

- Backup Systeme

Schutz durch IT-Monitoring, Agenten und Sensoren, Pen-Test

Das IT-Sicherheitskonzept flexpo Security der F&M Consulting basiert auf einer 3 Stufen Lösung mittels besonderer Hardware und Softwarekomponenten.

Überwachung (Stufe 1)

Eine IT Monitoring Software inkl. aller individuellen Konfigurationen sowie Datenbank und Meldeschnittstelle sind in einer gekapselten und mehrfach verschlüsselten Hardware CPU-Einheit untergebracht **(flexpo CPU Black Box).** Software Agenten und Sensoren kommunizieren mit allen zu schützenden IT Komponenten und vergleichen in Millisekunden-Takt Verhaltensmuster der Systeme und erkennen dadurch Abweichungen zu einem Normalbetrieb. Dadurch werden Meldungen in 3 Kategorien erzeugt. Die Eigensicherheit der Systeme (grün) , Auffälligkeiten (gelb) und ernste Bedrohungssituationen (rot).

Besonderheit: Die flexpo CPU Black Box beinhaltet neben einer IT Monitoring Software zahlreiche Sicherheitskomponenten, welche in einem gekapselten System untereinander interagieren und kontinuierlich an verschiedene Stellen melden oder alarmieren. Diese Komponenten agieren auch noch während ei-

nes Hackerangriffs und sind uneinnehmbar.

Die CPU verfügt über zahlreiche Schnittstellen und Ausbaustufen sodass auch Meldungen über Mobilfunk oder vorhandenen Gefahrenmeldesysteme (VDS) ausgelöst werden können.

Meldung (Stufe 2)

Eine **Security Applikation** in der Schnellstartleiste an allen PC Arbeitsplätzen informiert wie ein Messenger Dienst kontinuierlich über die Systemsicherheit. Des Weiteren werden den PC Benutzern aktuelle Informationen zur Bedrohungssituation durch kursierende Schadsoftware im Internet an den Arbeitsplatz gesendet und beinhalten aktuelle Empfehlungen und Verhaltensregeln. Auch ein Notfallmanagement ist integriert und verhilft im Ernstfall die richtigen Maßnahmen schnell und unverzüglich zu ergreifen. Dabei werden Sensibilisierungen zur Datensicherheit und Datenschutz als redaktioneller Dienst parallel an das Security Tool übermittelt. Somit wird auch ein Teil des Datenschutzmanagement als Auszug der Datenschutzgrundverordnung (DSGVO) an die EDV Benutzer herangetragen. Denn Cyberangriffe setzen häufig auf Erpressung, in dem ganze IT-Infrastrukturen inkl. Backups verschlüsselt werden sowie nach personenbezogenen Daten gezielt gesucht wird und Kopien dieser im Anschluss veröffentlicht werden.

Not Abschaltung (Stufe 3)

In einem bereits aktiven Bedrohungsfall, in dem beispielsweise alle Schutzmechanismen umgangen wurden, oder heimtückisch ein Identitätsdiebstahl des Administrators stattgefunden hat, kann nur noch eine Not Abschaltung der zentralen IT-Systeme schlimmeres verhindern. Zu diesem Zweck greift die **flexpo Security NOT-AUS Box** direkt in die zentrale Spannungsversorgung ein und unterbricht noch vor der USV alle Verbindungen.

Diese NOT-Abschaltung kann über verschiedene Mechanismen ausgelöst werden.

a.) Manuell vor Ort via NOT AUS Taste oder

b.) über einen Funk Standard per Mobilfunk (Code red).

Des Weiteren sind auch Anbindungen an Gefahrenmeldeanlagen über VDS-Protokoll möglich. Somit lassen sich auch weitere Services anbinden, welche z.B. eine 7/24 Überwachung aller generierten Gefahrenmeldungen sichten und im Notfall alarmieren. Auch eine Not Abschaltung (Code red) kann je nach Sicherheitskonzept auch ohne weitere Autorisierung automatisiert auslösen.

Integration der flexpo IT-Security Services.

Das Zusammenspiel dieser drei Sicherheitskomponenten wird dabei je nach Unternehmensgröße und IT-Sicherheitslevel über Service Packages individuell gestaltet. Die Hauptkomponente ist in einer **Hardware Security CPU** integriert und wird über eine definierte Laufzeit für den Klienten beigestellt. Die individuelle Einrichtung und Installation erfolgt nach einem festgelegten Sicherheitskonzept vor Ort. Dabei wird die CPU in einem eigenständigen Netzsegment eingerichtet und je nach Komplexität der IT-Infrastruktur in den Modulen Basic, Classic oder Premium konfiguriert. Die integrierte IT-Monitoring Software übernimmt dabei die Echtzeitüberwachung und generiert die Sicherheitsmeldungen an ein **Security Tool**. Dieses Security Tool (flexpo Service) arbeitet wie ein Messenger Dienst an den PC- Arbeitsplätzen und informiert die Benutzer über allgemeine und spezielle Bedrohungslagen. Somit werden auch die Benutzer an ihren Arbeitsplätzen in das IT-Sicherheitskonzept einbezogen.

Sicherheitsmeldungen über das Service Tool am Arbeitsplatz

Da das Einfallstor für Cyberangriffe über 90% über die Arbeitsplätze der User vollzogen wird, werden diese kontinuierlich über Sicherheitsmeldungen informiert und haben einen Zugriff auf eine potentielle oder reale Bedrohungslage sowie auf das einzuleitenden Notfallszenario.
Das **flexpo Security Tool** informiert des Weiteren auch proaktiv / redaktionell über aktuelle Cyber Bedrohungen und liefert Empfehlungen zum Schutz gegen drohende Angriffsversuche. (toxische eMails und Internet Seiten, falsche Identitäten und zahlreicher weiterer Phishing-E-Mails.

IT-Sicherheit ist ein Prozess in jedem Unternehmen welcher kontinuierlich den sich ändernden Sicherheitsbedrohungen angepasst werden muss. Die F&M Consulting bietet mit dem flexpo IT Security Package genau diesen Full Service Prozess für Unternehmen, die sich gegen die zunehmenden IT-Sicherheitsvorfälle schützen wollen.

Anfrage und Konditionen:

(3 Säulen IT-Sicherheitslösung)

Kontakt:

F&M Consulting
Technologie- und Organisationsberatung
für den Mittelstand

Telefon: +49 (0)203/608499-10
info@fundm.de
www.fundm.de
www.flexpo-security.de

Weitere Kernkompetenzen sind:

flexpo-Industrie
flexpo-Open Source
flexpo-Systemlösungen
IT-Outsourcing

Dienstleistung

flexpo IT Security Package 1

1. Einrichtung und Beistellung der flexpo IT-Security Black Box CPU
Einrichtungspauschale **(Aktive IT-Sicherheit)** und IT-Sicherheitsprüfung.

2.Festlegung der Security Level (**Basic, Classic, Premium**)
abhängig vom Sicherheitskonzept und Anzahl der Sensoren (Monitoring)

IT-Prävention Meldung, Warnung, Sicherheitstraining, für den
PC – Arbeitsplatz flexpo Security Tool
3.flexpo Security Tool (Messenger Dienst, monatliche Pauschale)

IT-Sicherheitsprüfung
4.Security Service (kont. Trimmung der Sensoren , Sicherheitsberatung)
Ticketminuten - Paket als Kontingent (480 Minuten)

flexpo IT Security Package 2 (Package 1 + Not Aus Box)
5.Einrichtung und Beistellung der flexpo IT-Security Not Aus Box
Einrichtungspauschale **(Aktive IT-Sicherheit)** und IT-Sicherheitsprüfung.

Weitere Dienstleistungen

- Krisenmanagement
- Sicherheitskonzepte, Prüfung Notfallszenario
- Erstellung von Alarm- und Meldeprozessen
- IT-Sicherheitsaudits
- Penetrationstest Infrastruktur +Backups
- Phishing Simulation - Cyber Angriff
- Rufbereitschaft, Sicherheitsbereitschaft
- Aktive Schadensbegrenzung (Einfallstor eruieren, schließen, Gegenmaßnahmen einleiten)
- Zertifizierte Externe Datenschutzbeauftragte, Externe IT-Sicherheitsbeauftragte
- IT Forensik , Gegenmaßnahmen bei Cyber Angriffen einleiten
- Check aller Systeme, Netze und Applikationen
- Entschlüsselung und Wiederherstellung
- IT-Gutachten für Versicherung und Behörden
- Unterstützung zum Wiederanlauf
- Anpassungen und Entwicklung von Schnittstellen zu Fremdsystemen