FI-TS 4D-Security
Immer, überall, sicher.

4D-Security ist die FI-TS Antwort auf alle Sicherheitsfragen. Denn 4D-Security arbeitet in vier Dimensionen gegen die potenzielle Bedrohung, ist also wirklich umfassend angelegt.

Die vier Dimensionen haben alles im Blick

4D-Security verzahnt die einzelnen Sicherheitsdimensionen und bietet sowohl situativ als auch zukunftsorientiert fundierte Analysen und Aktionen. So bietet 4D-Security zuverlässig den maximalen Schutz. Heute und in Zukunft.

Vorhersagen: Durch gezielten Informationsaustausch und Abgleich mit geeigneten Quellen wird die Liste der möglichen IoCs (Indicators of Compromise) permanent erweitert.

Vorbeugen: Durch leistungsstarke Sicherheitslösungen werden IT-Systeme und Geschäftsprozesse abgesichert und Sicherheitsvorfälle verhindert.

Reagieren: Mittels Security-Incident-Prozess werden Sicherheitsvorfälle analysiert, bewertet und durch geeignete Maßnahmen eingedämmt oder behoben.

Erkennen: Permanentes Schwachstellenmanagement und Security-Monitoring ermöglichen es, Sicherheitslücken sofort zu erkennen.

Vorhersagen | **Vorbeugen** | **Erkennen** | **Reagieren**

Security Incident and Event Management (SIEM)

Malware Information Sharing Platform (MISP)

Security- und Compliance-Reports

Schwachstellenmanagement

Endpoint Protection

Data Loss Prevention

Secure E-Mail Gateway

Zugriffs- und Nutzungskontrolle

Network Access Control

Verschlüssungssysteme/ Krypto-Management

Firewall-Management

Compromise Assessment

Forensische Untersuchungen

Penetration-Testing

Distributed Denial of Service-Mitigation (DDos)

Intrusion-Detection-Systeme (IDS)

Intrusion-Prevention-Systeme (IPS)

Ihre Vorteile durch FI-TS 4D-Security

- Bedrohungen schnell erkennen
- Angriffe effektiv verhindern und abwehren
- Akteure und Vorgehensweisen kennen und verstehen
- Abwehrtechniken weiterentwickeln
- Rechtssicherheit erhalten
- Use-Case-Entwicklung im SIEM zur gezielten Analyse von Angriffsvektoren in Bezug auf Kundenumgebungen
- Transparenz und Planungssicherheit für rechtliche Prüfungen bzgl. Use-Case-Regel-Entwicklung
- Implementieren eigener Use-Cases-Regeln für dedizierte Kunden-Systeme möglich
- Kostengünstiger und planbarer Betrieb
- Security-Spezialisten an Ihrer Seite

Die zentralen Bausteine der FI-TS 4D-Security

SIEM – Security Incident and Security Event Management

Die Basis umfassender Sicherheit

Der Grundbaustein von FI-TS 4D-Security ist das SIEM. Es vereinigt eine umfassende Perspektive mit hoher Geschwindigkeit: Vom Betrieb bis zur Cybercrime-Abwehr reicht sein Anwendungsgebiet, und es ermöglicht ein überaus schnelles Reagieren auf Sicherheitsvorfälle.

Im Kern funktioniert das SIEM wie folgt: Zunächst werden auf Basis des Security Operation Managements (SOM) Regeln sogenannte Use-Cases zum Erkennen von möglichen Sicherheitsvorfällen erstellt. Die zugehörigen Meldungen werden im Anschluss stets von FI-TS Security-Spezialisten bearbeitet, so dass bei Eintritt eines Sicherheitsvorfalls unmittelbar fundierte Einschätzungen vorgenommen und zur Eindämmung bzw. Beseitigung des Sicherheitsvorfalls sinnvolle Maßnahmen eingeleitet werden können.

MISP – Malware Information Sharing Platform

Bester Schutz durch eine starke Community

Bedrohungen noch schneller erkennen und Angriffe noch besser abwehren – dafür hat FI-TS die Plattform MISP in sein Cyber Defense Center integriert. So nutzen wir die Kraft der Gemeinschaft, um Akteure und Vorgehensweisen verlässlicher zu verstehen, hinsichtlich Malware stets auf dem aktuellsten Stand zu sein und Abwehrtechniken weiterzuentwickeln.

Gepflegt wird die Anti-Schadsoftware-Plattform von einer breit aufgestellten, weltweiten Community. Und getragen von dem Gedanken, dass hier alle profitieren, wenn sie ihr Wissen teilen: So erhalten Sie einen starken Boost für eine automatisierte und qualifizierte Cyber-Abwehr und mithin ein echtes Plus an Sicherheit.

Security- und Compliance-Reports

Um wichtigen Anforderungen sicher gerecht zu werden

Reports sind für so essenzielle Bereiche wie Sicherheit und Compliance heute unerlässlich. Insbesondere gilt dies in der hochregulierten, sehr kapitalstarken sowie außerordentlich dynamischen Finanz- und Versicherungsbranche. Wir unterstützen Sie mit wichtigen Reports zu zentralen Themen, die rechtliche Vorgaben, Unternehmensrichtlinien und Steuerungsmanagementaspekte (unternehmensintern, gegenüber dem Provider etc.) berücksichtigen. Mit einem individuell zugeschnittenen Security- und Compliance-Reporting von FI-TS sorgen Sie für eine weite und fachkundige Perspektive in Ihrem Unternehmen sowie stets einen aktuellen Überblick. So kann Ihre Organisation, etwa gegenüber Finanzaufsichtsbehörden, leicht alle notwendigen Nachweise erbringen.

Schwachstellenmanagement

Potenzielle Angriffspunkte erkennen und möglichst beseitigen

Für die proaktive Prävention ist das Schwachstellenmanagement ein wesentlicher Bestandteil. Es trägt entscheidend dazu bei, Cyber-Angriffe möglichst zu unterbinden, indem es Angriffsrisiken minimiert. Für ein effektives Schwachstellenmanagement greifen wir auch auf bewährte und spezialisierte Quellen zu, etwa: S-CERT des SIZ (Informatikzentrum der Sparkassenorganisation GmbH), KRITIS-Meldungen (KRITIS = kritische Infrastruktur; entsprechende Betreiber unterliegen speziellen Cyber-Security- und Meldepflichten) und Vulnerability-Datenbank (Gefahren-/Schwachstellen-Informationen, rund um die Uhr aktualisiert). Bei allen durch FI-TS betreuten Systemen werden Schwachstellen im Rahmen des FI-TS Patch-Managements behoben.

Endpoint Protection

Mehr als nur Virenschutz

Dass die Endgeräte im Netzwerk sicher sind – also etwa Laptop, Smartphones, Tablets und IoT-Geräte (IoT = Internet of Things) – nicht gehacked oder von Viren befallen werden, dafür sorgt die sogenannte Endpoint Protection. Präventive, detektive und reaktive Maßnahmen werden hier durch technische Lösungen realisiert, und zwar durch dezentrale sowie zentralisierte. Zu den dezentralen Lösungen gehören etwa: Härtung von Endgeräten (wie z. B.: es kann nur benötigte und vorab genehmigte Software genutzt werden), Viren- und Malware-Schutz, Client Firewalls, Zugriffskontrolle, Sandboxing (das Schaffen von isolierten Bereichen) und URL-Filter. Und zu den zentralisierten Sicherheitsmaßnahmen gehören unter anderem: Firewalls, Zugriffssteuerungen und Intrusion-Detection- oder Intrusion-Prevention-Systeme. Die Endpoint Protection schützt dabei letztlich nicht nur die Endpunkte eines IT-Netzwerks, sondern über sie entscheidend auch das ganze Netzwerk, also die gesamte IT-Infrastruktur mit allen IT-Systemen.

Data Loss Prevention

Geistiges Eigentum und unternehmenskritische Daten vor Diebstahl und Verlust schützen

Datendiebstahl verhindern – darum geht es bei DLP. Mit der richtigen Organisation, geeigneten Workflows sowie dem gezielten Einsatz entsprechender Methoden und Tools werden insbesondere kritische Unternehmensdaten vor dem Zugriff durch Unberechtigte geschützt. Um einen unerwünschten Datenabfluss zu unterbinden und so einen zuverlässigen Schutz des geistigen Eigentums sowie weiterer sensibler Daten zu erreichen, sind zunächst die schützenswerten Daten zu identifizieren und ist deren Kompromittierung zu vereiteln. Folgerichtig müssen alle zugehörigen Parameter, also etwa auch die unterschiedlichen Zustände der Datensätze (in Benutzung, in Bewegung, im Ruhezustand) für eine effektive DLP mitberücksichtigt werden. Grundlegend unterscheiden lassen sich DLP-Lösungen dabei hinsichtlich ihres Einsatzgebietes: Enterprise-DLP-Lösungen sind im Regelfall umfassende Tools, die unternehmensweit Daten in jedem dieser Zustände schützen. Integrierte DLP-Lösungen fokussieren dagegen nur auf einen bestimmten Status und meist nur in einem definierten Unternehmensbereich. FI-TS hilft Ihnen bei der Auswahl und dem passgenauen Zuschneiden der Lösung für Ihr Unternehmen.

Secure E-Mail Gateway

Den E-Mail-Versand über Verschlüsselung und Signatur sicher gestalten

Damit auch wirklich vertraulich bleibt, was der Sache nach vertraulich ist, und Schadattacken vereitelt werden: Das Secure E-Mail Gateway von FI-TS sorgt für eine sichere E-Mail-Kommunikation. Denn E-Mails können verschlüsselt an unternehmensexterne sowie -interne Empfänger versandt werden. Und natürlich lassen sie sich über diesen sicheren Kommunikationskanal auch verschlüsselt empfangen. Dabei gilt: E-Mails, die über das Internet geroutet werden, werden am Gateway zentral verschlüsselt und signiert. Kurz zusammengefasst: Der Service Das Produkt Secure E-Mail Gateway von FI-TS beinhaltet die Nutzung eines zentralen Gateways mit den verschiedensten Verschlüsselungsmethoden und erhöht maßgeblich die Sicherheit in der Kommunikation.

Zugriffs- und Nutzungskontrolle

Mehr Sicherheit durch passgenauen Zugang zu Ihren Diensten

Dass jeder an die Daten, Funktionen und Systeme herankommt, die er benötigt, und zugleich unberechtigte und ungewollte Zugriffe verhindert werden: Das ist der Sinn von Identity and Access Management (IAM). Die rollenbasierte User- und Rechteverwaltung von FI-TS umfasst dabei den ganzen User-Lifecycle und berücksichtigt stets die vollständige Unternehmensarchitektur. Das Produkt IAM von FI-TS beinhaltet im Kern: Segregation of Duties (SoD, Funktionstrennung), Rollenmodellierung und Rezertifizierung (die Zertifizierung wird in fest implementierten Prozessen regelmäßig überprüft und ggf. erneuert). Durch die Rezertifizierung wird verhindert, dass ehemalige Funktionsträger dauerhaft mit gültigen „Schlüsseln“ herumlaufen und somit inhärente Sicherheitsrisiken darstellen. Rollenmodellierung und SoD zielen darauf ab, dass anwenderspezifisch alle benötigten Zugriffe möglich sind, alle nicht benötigten jedoch nicht.

Network Access Control

Nur Hardware im Netzwerk zulassen, die geprüft und gebilligt ist

Fremde Hardware im Netz ist ein Sicherheitsrisiko. Dabei muss es hier nicht einmal um gezielte Angriffe von außen gehen. Oft ist es einfach so: Mitarbeiter nutzen private Endgeräte – und schaffen so aus reiner Unbedachtheit Einfallstore für Schadsoftware und Co. Mit der Network-Access-Control-Lösung von FI-TS wird hier ein starker Schutz bereitgestellt: Ausschließlich autorisierte Endgeräte können einen Zugang zum Netzwerk erhalten. Nur was geprüft und gebilligt ist, kommt also hinein. Das bringt ein bedeutendes Plus an Schutz – gerade gegen Unachtsamkeit aus den eigenen Reihen und also bei einem Thema von großer Relevanz, dem aber häufig zu geringe Beachtung geschenkt wird.

Verschlüssungssysteme/Krypto-Management

Sensible Daten im Tresor sichern – regelungskonform und komfortabel

Sensible Daten gilt es zu schützen. Oft wird hier auch ein hoher Aufwand betrieben, doch entscheidende Zugangsmöglichkeiten bleiben unbeachtet. Was aber nützen selbst die besten Sicherungssysteme, wenn man etwa den Zugangsschlüssel offen herumliegen lässt? Genau dieser Frage nimmt sich das Krypto-Management an. Bei ihm geht es darum, sensible Daten – wie Passwörter, Keys und sonstige Zugangsberechtigungen – zu verschlüsseln und sicher zu verwahren. Oder anders ausgedrückt: Ihre Wertsachen kommen in den Tresor, und diesen können auch wirklich nur die Mitarbeiter öffnen, die Zugang zu ihm haben sollen.

Im Rahmen des Krypto-Managements von FI-TS werden dabei selbstredend alle Compliance- und Sicherheitsanforderungen eingehalten. Dazu wird ein komfortables Handling von uns gewährleistet.

Firewall-Management

Der Brandschutz am Eingang

Eine Firewall dient als Sicherung am Systemeingang. Vergleichbar ist sie mit einer Brandschutztür, die man beim Betreten eines Gebäudes passieren muss: Im Alltag fällt sie einem kaum auf, doch sie verhindert durch gezielte Zugangsbegrenzungen bzw. -blockaden schlimme Unfälle und Verluste, ist also im Fall des Falles extrem wichtig. Im Kern leisten sie dies: Firewall-Systeme schützen den Datenverkehr auf Basis von Quell- und Zieladressen sowie genutzten Diensten. Und die interne Struktur des Netzwerks dahinter wird gegenüber Dritten verborgen. Weit verbreitet und bekannt sind generelle Firewalls, neben ihnen gibt es auch noch spezialisierte Firewall-Systeme, etwa Web-Applikations-Firewalls (WAF, gezielter Schutz für Web-Applikationen). Für die FI-TS Firewall-Produkte gilt: Sie sind grundsätzlich in unterschiedlichen Ausprägungen und Servicestufen erhältlich sowie auch an Kundenstandorten direkt einsetzbar. Sie werden bedarfsgerecht ausgewählt und kundenspezifisch angepasst. Zudem sind sie umfassend und technisch auf dem aktuellsten Stand, so ist zum Beispiel die FI-TS WAF zusätzlich mit einem DDoS-Angriffsschutz ausgestattet.

Compromise Assessment

Hackerspuren finden und für die eigene Sicherheit nutzen

Ist ein Hackerangriff erfolgt, so ist dieser damit aus IT-Sicht noch nicht vorbei: Hacker hinterlassen Spuren, und wer sie zu lesen imstande ist, der kann sich künftig noch besser schützen. Compromise Assessment, fahndet gezielt nach Spuren eines Cyber-Angriffes – und stellt so auch die ideale Ergänzung zum allgemeinen Schwachstellenmanagement und zum regelmäßigen Pentesting dar. Unser APT-Scanner (APT = Advanced Persistant Threat, also: fortentwickelter Scanner gegen Bedrohungen) findet die Spuren, und unsere spezialisierten Mitarbeiter bewerten sie dann und leiten Maßnahmen aus ihnen ab.

Penetration-Testing

Der Härtetest für IT-Systeme

Nur wer das Penetration-Testing besteht, ist auch tatsächlich wirklichkeitstauglich. FI-TS bietet deswegen Pentest as a Service an, also die professionelle Simulation von Cyberangriffen. Dabei verfolgen wir stets zwei Ziele: Risiken minimieren und das Erfüllen regulatorischer Anforderungen nachweisen. Bei uns erhalten Sie den kompletten Pentest-Service aus einer Hand: FI-TS übernimmt Organisation, Koordination, Ergebnisaufbereitung und nachgelagertes Schwachstellenmanagement. Die Tests selbst werden von unabhängigen, neutralen Pentestern durchgeführt.

Intrusion-Detection- und Prevention-Systeme

Schädliche Aktivitäten entdecken und abwehren

Einbruchs- und Manipulationsversuche automatisch zu erkennen und so Datennetzwerke und Serversysteme abzusichern, das ist die Aufgabe von IDS- und IPS-Lösungen. Reine Intrusion-Detection-Systeme (IDS) dienen lediglich der Angriffserkennung. Intrusion-Prevention-Systeme (IPS) bieten neben der IDS-Funktion auch die Möglichkeit, erkannte Angriffe gleich abzuwehren. FI-TS bietet ausgereifte und aktualisierte IDS-/IPS-Sensoren für Netzwerke und IDS-/IPS-Hostsensoren für die gezielte Überwachung von Serversystemen werden hier zum Beispiel in die Sicherung von Kundensystemen eingebunden.

Forensische Untersuchungen

Sicherheitsvorfälle erkennen und ausführlich analysieren

Ähnlich wie man es aus Krimis kennt, gibt es auch im IT-Bereich forensische Untersuchungen: Sie definieren nach einer erfolgten Tat (Kompromittierung) den Grund (root cause), die Auswirkung, Ausbreitung und den eingetretenen Schaden eines Vorfalles. Auf Wunsch erfolgt dies gerichtsverwertbar für den Kunden.

Der abschließende forensische Bericht erläutert in der Management-Summary und, gerichtlich verwertbar in technischer Tiefe, alle Analyseschritte sowie die damit einhergehende Schlussfolgerungen im Detail.

DDoS-Mitigation

Effektiver Schutz vor Überlastungsangriffen auf IT-Dienste

Den Server in die Knie zwingen, indem man ihn mit Anfragen quasi bombardiert, und so eine Webseite aus dem Netz drängen: So funktioniert im Kern ein DDoS-Angriff. Man kennt das aus den Nachrichten, zum Beispiel wird über DDoS-Angriffe berichtet, wenn Anonymous gezielt gegen eine Organisation vorgegangen ist. Diese spezielle Art der Cyberattacke ist aber keineswegs auf wenige spektakuläre Vorfälle begrenzt, sie findet ganz alltäglich und in großer Breite statt. Und es geht auch nicht nur um Webseiten und Server: Nein, praktisch jede Art von IT-Infrastruktur und IT-Dienstleistung kann so angegriffen werden.

Kontakt

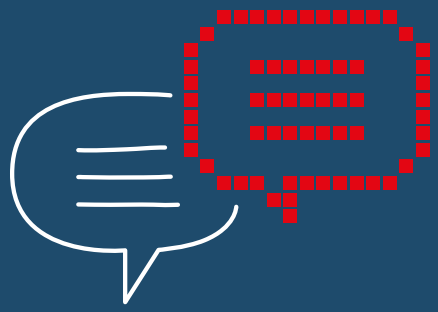
Schützen Sie ihre IT mit den Security-Lösungen von FI-TS. Unser Ziel ist die Sicherstellung und kontinuierlichen Erweiterung sämtlicher Überwachungs- und Schutzmaßnahmen. Dafür haben wir Spezialisten in unserem Cyber Defense Center für Sie im Einsatz.

Über Finanz Informatik Technologie Service (FI-TS)

Die Finanz Informatik Technologie Service GmbH & Co. KG (FI-TS) ist ein etablierter IT-Partner der Finanzwirtschaft und größter IT-Dienstleister für Landesbanken. Als Tochter der Finanz Informatik (FI) und Teil der Sparkassen-Finanzgruppe unterstützt der IT-Provider private und öffentliche Banken, Versicherungen und Finanzdienstleister mit standardisierten IT-Dienstleistungen.

FI-TS versteht sich als Brückenbauer, der seine Kunden bei ihren Digitalisierungsvorhaben begleitet. Auf Basis einer integrierenden IT-Service- Plattform mit Leistungen vom klassischen Rechenzentrums- betrieb bis hin zu Public-Cloud-Produkten und Services wie Compliance, Providermanagement, Transition, Transforma- tion, Beratung ermöglicht das Unternehmen seinen Kunden die digitale Transformation. FI-TS bringt langjährige Erfahrun- gen aus der Finanzbranche in Kundenbeziehungen ein und richtet seine Services an den regulatorischen Anforderungen der Branche aus – „IT made for Banking and Insurance“.

Die hundertprozentige Tochter der Finanz Informatik hat ihre Unternehmenszentrale in Haar bei München. Dort und an den Standorten Hannover, Nürnberg, Offenbach und Stuttgart (Fellbach) arbeiten rund 1.000 Mitarbeiterinnen und Mitarbeiter. Der Jahresumsatz beträgt rund 400 Millionen Euro (2021).



Finanz Informatik Technologie Service

Richard-Reitzner-Allee 8, 85540 Haar
+49 89 94511-0
anfragen@f-i-ts.de
www.f-i-ts.de

finanz **informatik**
technologie service