
FI-Gruppe
FI-TS
DIE VIER DIMENSIONEN DER SICHERHEIT
Sicherheit ist eine Prämisse der Banken-IT. Dementsprechend professionell organisiert die FI-Gruppe ihre Maßnahmen zur Abwehr von Cyber-Risiken. Die IT der Sparkassen schützt die Finanz Informatik (FI) unter anderem mit ihrem Cyber Defence Center. Für die Sparkassen-Finanzgruppe bietet sie ebenfalls Security Services an.

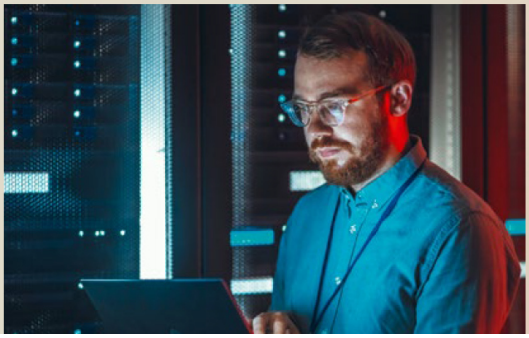
Individuelle Sicherheitsanforderungen von Landesbanken und Verbundunternehmen, die auch Anwendungen einsetzen, die über den FI-Standard hinausgehen, bedient die FI-Tochter FI-TS mit umfassenden Security-Services, die sie in der Familienmarke FI-TS 4D-Security zusammenfasst.

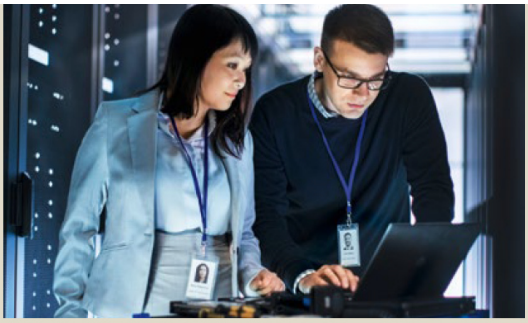
Keine Kompromisse

Das ist das Leitmotiv der FI-Gruppe bei der Prävention, dem Erkennen und dem Abwehren von Sicherheitsrisiken. Für einen lückenlosen Schutz ihrer Kunden bieten sowohl die FI als auch FI-TS umfassende Services durch professionell geschulte Sicherheitsexperten an, die die Anwendungen und die IT-Infrastruktur absichern. Dafür stehen FI und FI-TS im regelmäßigen Austausch und stimmen ihr Portfolio für diese Kunden aufeinander ab. Auf diese Weise können gemeinsame Kunden wie etwa Landesbanken und Verbundunternehmen einen Schutz auf höchstem Niveau erhalten.

FI-TS 4D-Security verzahnt die Sicherheitsdimensionen »Vorhersagen«, »Vorbeugen«, »Erkennen« und »Reagieren«. »Vorhersagen« bedeutet, dass FI-TS den gezielten Informationsaustausch übernimmt und steuert. Dafür bezieht sie sicherheitsrelevante Informationen von relevanten Quellen und nutzt diese Informationen, um mögliche Bedrohungen vorherzusagen und zu verhindern. Damit wächst im Ergebnis eine Liste an möglichen IoCs (Indicators of Compromises), auf die dann weitere Maßnahmen abgestimmt werden.

Im Bereich »Vorbeugen« geht es darum, dass FI-TS mit leistungsstarken Sicherheitslösungen die IT-Systeme und Geschäftsprozesse ihrer Kunden schützt. So betreibt der Provider eine weitreichende Prävention zu möglichen Sicherheitsvorfällen. Bei der dritten Sicherheitsdimension »Erkennen« unterstützt FI-TS seine Kunden durch ein permanentes Schwachstellenmanagement und Security-Monitoring dabei, Sicherheitslücken frühzeitig zu erkennen. Im Zusammenhang mit »Reagieren«, der vierten Dimension, bedeutet dies, dass FI-TS bei ihren Kunden einen Security-Incident-Prozess zur Behandlung von Sicherheitsvorfällen implementiert. Dies ist eine wichtige Voraussetzung dafür, Sicherheitsvorfälle zu analysieren und zu bewerten, um dann durch geeignete Maßnahmen den Vorfall einzudämmen oder zu beheben.





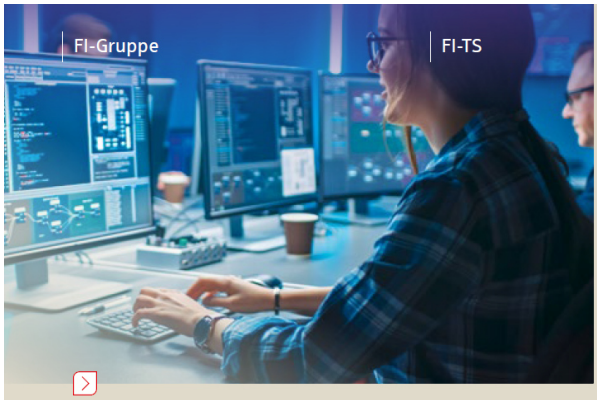
Leistungsfähiges SIEM ist Grundlage für die 4D-Security

Das »Security Incident and Security Event Management« (SIEM) ist der Grundbaustein von FI-TS 4D-Security. Es ermöglicht das schnelle Reagieren auf Sicherheitsvorfälle in allen Bereichen, angefangen vom Betrieb bis zur Cybercrime-Abwehr. FI-TS erstellt auf Basis des Security Operation Managements (SOM) sogenannte Use Cases zum Erkennen von möglichen Sicherheitsvorfällen inklusive zugehöriger Meldungen. Das ermöglicht es den Security-Spezialisten des Providers, erkannte Sicherheitsvorfälle fundiert einzuschätzen und sinnvolle Maßnahmen zur Eindämmung beziehungsweise Behebung einzuleiten.

A und O eines umfassenden Sicherheitsmanagements ist das präzise Vorhersagen sicherheitsrelevanter Gefahren. Dafür hat der Provider eine Malware Information Sharing Platform in das FI-TS-eigene Cyber Defense Center integriert. Dies hilft, aufkommende Bedrohungen schnell zu erkennen und Angriffe noch besser abzuwehren. Mit der Plattform sichert sich der Provider den Zugang zu einer starken Gemeinschaft. Diese arbeitet gemeinsam daran, Angreifer und deren Vorgehensweisen verlässlicher zu verstehen. Dadurch können passgenaue Abwehrtechniken weiterentwickelt werden. Zudem erstellt FI-TS Reports zu zentralen Themen, die rechtliche Vorgaben, Unternehmensrichtlinien und Steuerungsmanagementaspekte (unternehmensintern, gegenüber dem Provider etc.) betreffen. Die Reports erfüllen einerseits die regulatorischen Vorgaben, die die Aufsicht an die Finanz- und Versicherungsbranche stellt und schaffen andererseits die Möglichkeit, aus Gefährdungssituation für die Zukunft zu lernen.

Breiter Strauß an vorbeugenden Security-Services

Neben präzisen Vorhersagen stellt das Vorbeugen von Sicherheitsvorfällen den wirksamsten Schutz vor Cyberangriffen dar. Hier bietet FI-TS einen breiten Strauß an Security-Services, mit denen Finanzdienstleister sich bestmöglich absichern können. Die FI-Tochter setzt durch ein professionelles Schwachstellenmanagement auf proaktive Prävention. Damit minimiert sie Angriffsrisiken. Im Rahmen des FI-TS-Patch-Managements werden mögliche Schwachstellen in allen durch den Provider betreuten Systemen behoben. Als weitere vorbeugende Maßnahme sichert FI-TS Endgeräte wie Laptops, Smartphones, Tablets und IoT-Geräte (IoT = Internet of Things) im Netzwerk der Kunden ab, damit diese nicht gehackt oder von Viren befallen werden. Damit schützt der Provider zugleich das ganze Netzwerk, also die gesamte IT-Infrastruktur mit allen IT-Systemen.



Um geistiges Eigentum sowie unternehmenskritische Daten vor Diebstahl und Verlust zu schützen, bietet FI-TS nicht nur einen passenden organisatorischen Rahmen, sondern auch spezielle Workflows, Methoden und Tools. Diese schützen kritische Unternehmensdaten vor unberechtigtem Zugriff. Kunden können ein Secure E-Mail Gateway nutzen, um die E-Mail-Kommunikation abzusichern. Damit können E-Mails sowohl intern als auch extern verschlüsselt versandt und empfangen werden. Das Identity and Access Management (IAM) stellt sicher, dass nur berechtigte Personen auf Systeme und Dateien zugreifen können. Mithilfe einer rollenbasierten User- und Rechteverwaltung steuert FI-TS ganzheitlich den Zugriff auf die gesamte Unternehmensarchitektur im Sinne eines User-Lifecycles. Durch diese Maßnahmen wird gewährleistet, dass nur autorisierte Personen Zugriff auf die relevanten Systeme und Daten haben, was Sicherheit und Vertraulichkeit der Unternehmensinformationen erhöhen.

Um sicherzustellen, dass nur zugelassene und geprüfte Hardware im Netzwerk eingesetzt wird, verwendet FI-TS eine Network-Access-Control-Lösung. Sensible Daten wie Passwörter, Keys und Zugangsberechtigungen werden durch Krypto-Management verschlüsselt und sicher verwahrt. Hierbei werden alle geltenden Compliance- und Sicherheitsanforderungen eingehalten, um ein komfortables Handling zu gewährleisten. Außerdem schützt FI-TS den Datenverkehr seiner Kunden über dedizierte Firewall-Systeme, die sowohl generelle als auch spezialisierte Firewall-Systeme wie Web-Applikations-Firewalls (WAF) umfassen. Durch diese Maßnahmen wird eine umfassende Sicherheit im Netzwerk gewährleistet. Das trägt dazu bei, Unternehmensdaten bestmöglich zu schützen.

Analyse von Hackerattacken verhilft zu besserem Schutz

Doch auch der beste Schutz durch vorbeugende Maßnahmen entbindet nicht davon, auf der Hut zu bleiben. Es gilt, kompromittierende Handlungen und Angriffe schnellstmöglich zu erkennen. Über den Security-Service »Compromise Assessment« analysiert FI-TS erfolgte Hackerangriffe. Der Provider analysiert hinterlassene Spuren und leitet daraus Maßnahmen ab, um die Kunden noch besser zu schützen. Compromise Assessment ergänzt das Schwachstellenmanagement und die regelmäßigen Pentestings. Letztere sind simulierte Angriffe aus externen oder internen Quellen, mit denen die Sicherheit von Webanwendungen, Apps, Netzwerken und Infrastrukturen überprüft und etwaige Schwachstellen aufgedeckt werden. FI-TS bietet seinen Kunden Pentest as a Service an. Dabei simuliert der Provider professionelle Cyberangriffe. Das minimiert Risiken nachweislich regulatorischer Anforderungen. Die Tests werden von unabhängigen, neutralen Pentestern durchgeführt.

FI-TS beherrscht nicht nur die Königsdisziplin, frühzeitig Cyberattacken zu erkennen, sondern kann auch schnell und effektiv darauf reagieren. Dazu nutzt der Provider Intrusion-Detection- und -Prevention-Systeme, die automatisch Einbruchs- und Manipulationsversuche erkennen und Datennetzwerke sowie Serversysteme entsprechend absichern. FI-TS stellt seinen Kunden hochentwickelte IDS-/IPS-Sensoren für die Überwachung von Netzwerken sowie IDS-/IPS-Hostsensoren für die gezielte Überwachung von Serversystemen zur Verfügung. Diese Sensoren werden kontinuierlich aktualisiert, um stets auf dem neuesten Stand der Technik zu bleiben.

Falls es trotz aller Maßnahmen zu einem Sicherheitsvorfall kommt, steht FI-TS seinen Kunden zur Seite und unterstützt bei den sogenannten forensischen Untersuchungen. Dabei arbeiten spezialisierte forensische Experten daran, den Ursprung des Vorfalls, dessen Auswirkungen, Ausbreitung und den entstandenen Schaden zu definieren. Auf Wunsch können diese Untersuchungen gerichtsverwertbar durchgeführt werden. FI-TS bietet außerdem seinen Kunden den Security Service »DDoS-Mitigation« an, der hilft, die täglich in der Finanzwirtschaft auftretenden DDoS-Angriffe erfolgreich zu bewältigen.