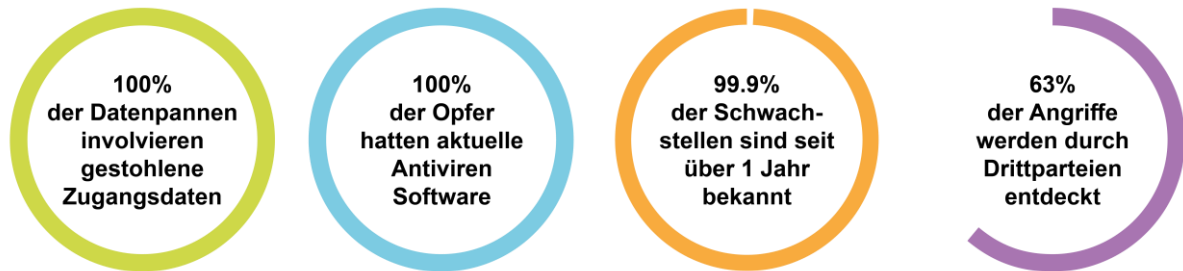


FS Cyber Control

205 Tage braucht es, um gezielte Angriffe zu entdecken!



Swiss Made IT-Schwachstellen Management für kleine und mittlere Unternehmen

Wie gut kennen Sie Ihre IT-Infrastruktur? Sind Ihre Daten wirklich sicher? Kennen Sie die Schwachstellen und deren Risiko?

In Ihrer IT-Infrastruktur befinden sich mit ziemlicher Sicherheit Schwachstellen, welche von Angreifern ausgenutzt werden können. Meist werden solche Angriffe viel zu spät bemerkt und der Schaden, sei es ein Informationsdiebstahl oder Imageverlust, kann unternehmenskritisch sein. Meldungen von Schaden verursachenden Angriffen auf Firmen nehmen kontinuierlich zu und der Höhepunkt dieser Attacken scheint noch lange nicht erreicht zu sein.

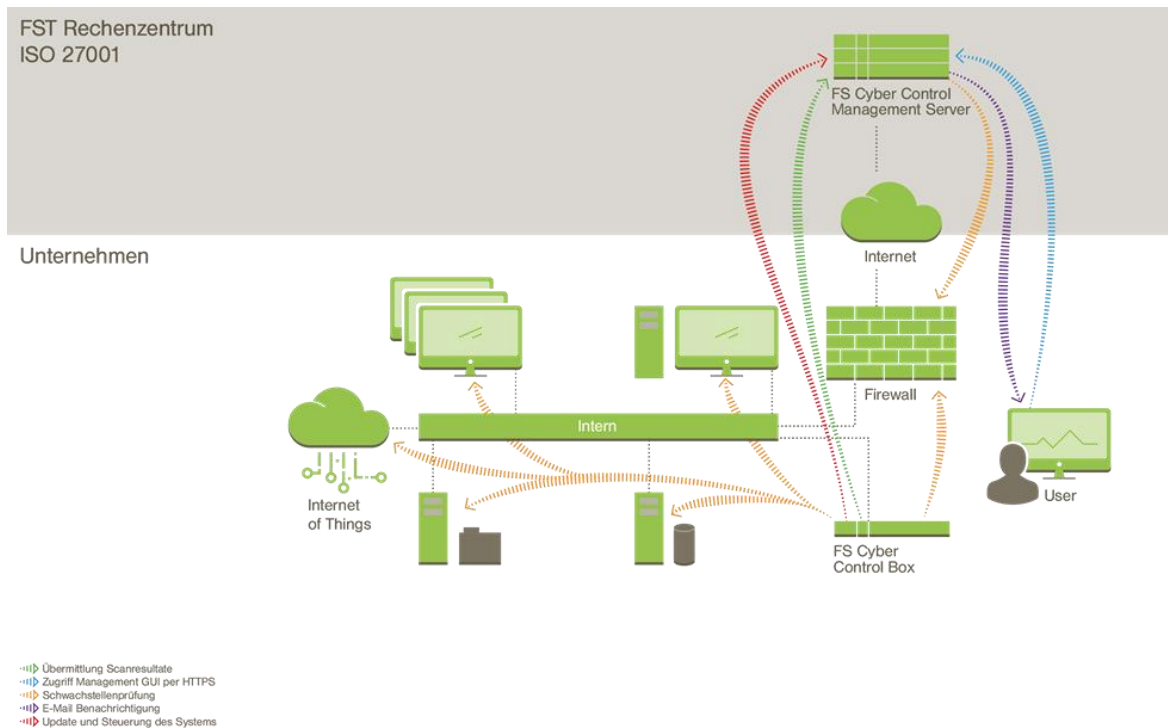
Mit FS Cyber Control, unserer Swiss Made Schwachstellenprüfung, kann das Risiko von unerlaubten Zugriffen massiv reduziert werden.

FS Cyber Control wurde speziell auf die Bedürfnisse von kleinen Unternehmen zugeschnitten und ist in der Lage bis zu 100 Systeme (IP-Adressen) zu überwachen.

- Identifiziert IT-Schwachstellen und zeigt Lösungen auf, um diese zu beheben
- Prüft das interne IT-Netzwerk und den externen Zugriff aus dem Internet regelmässig, umfassend und vollautomatisch
- Die daraus resultierenden Reports sind für alle, unabhängig von der Geschäftsebene und IT-Kenntnissen, einfach zu verstehen, damit schnell die richtigen Massnahmen eingeleitet werden, um die Risiken zu minimieren.
- Nahtlose, einfache und schnelle Integration in die bestehende IT-Umgebung

Nehmen Sie Ihre Verantwortung wahr, einen optimalen Schutz der IT-Infrastruktur und der Daten zu gewährleisten – FS Cyber Control unterstützt Sie dabei.

Funktionsweise



Wie funktioniert es?

Die FS Cyber Control Box verbindet sich regelmässig mit dem FS Cyber Control Management Server um die tagesaktuelle Updates zu Schwachstellen, Signaturen und dem System zu erhalten. Dafür lässt der Kunde eine geschützte Kommunikation zum FS Cyber Control Management Server zu.

Die Inventarisierung erfolgt täglich und die Security-Scans wöchentlich im internen Netzwerk und auf die öffentliche(n) IP-Adresse(n) des Internetanschlusses. Während dem Prüfzeitpunkt werden aktive und im Netzwerk erreichbare Systeme identifiziert und untersucht, bis die maximale Anzahl der zu prüfenden Systeme gemäss der Lizenz erreicht ist.

Als Ergebnis der Prüfung erhalten Sie drei verschiedene Berichte, welche auf die Adressanten Geschäftsleitung, IT Management und operative IT zugeschnitten sind. Sie bestimmen, wann wer welche Berichte erhält um einen optimalen Informationsfluss zu gewährleisten. Der GL Bericht zeigt anhand einer Ampel, wie es um ihre IT-Sicherheit steht. Der IT Management Bericht zeigt visuell die verschiedenen Herausforderungen. Im Massnahmekatalog für die operative IT werden Vorschläge zur Behebung der Schwachstellen detailliert aufgeführt.

Funktionen & Nutzen



Überwachung

Systematische IT-Überwachung des Inventars und Schwachstellenprüfung.



Sicherheit

Erhöhung der Sicherheit durch richtige Massnahmen zum IT-Schutz.



Zertifizierung

Zertifizierung und Qualitätsprüfung der IT-Infrastruktur.



E-Mail Benachrichtigung

Sofortige E-Mail Benachrichtigung bei neu entdeckten Schwachstellen.



Intuitiv

Durch Benutzerfreundlichkeit schnell und einfach an die richtigen Informationen gelangen.



Reports

Einfach zu vertsehende Dokumentation und regelmässiges Reporting.

Warum wird Vulnerability Management betrieben?

Hauptsächlich wird Vulnerability Management betrieben um eine Steigerung der IT-Sicherheitsqualität zu erreichen.

Schwachstellen werden frühzeitig erkannt, bevor sie ausgenutzt werden und einen Schaden verursachen. Unter anderem verursacht man mit Vulnerability Management langfristig Kosteneinsparungen durch Prozessoptimierungen zu erreichen. Gleichzeitig wird es genutzt, um eine Sicherheitslandkarte Ihrer Infrastruktur zu erstellen, sprich eine Inventarisierung Ihrer Systeme und den darauf laufenden Diensten.

Preise & Vertragskonditionen

Preise

Systeme (IP's)	Setup Kosten (einmalig)	Kosten pro Jahr (wiederkehrend)	Kosten pro Monat (wiederkehrend)
10	CHF 295.–	CHF 895.–	CHF 74.60
25	CHF 395.–	CHF 1'895.–	CHF 157.90
50	CHF 495.–	CHF 2'995.–	CHF 249.60
100	CHF 595.–	CHF 4'995.–	CHF 416.25

Vertragsdauer

- 1 Jahr, kündbar drei Monate auf Ende jedes Monats nach Ablauf der Mindestvertragsdauer von 1 Jahr.
- 3 Jahre, kündbar drei Monate auf Ende jedes Monats nach Ablauf der Mindestvertragsdauer von 3 Jahren.

Bei Abschluss eines Dreijahresvertrags mit Vorauszahlung wird die Setupgebühr erlassen.

Zahlungsmodalitäten

Die Zahlung kann quartals- oder jahresweise erfolgen. Bei Quartalsrechnung kommen pro Rechnung CHF 20 hinzu.

Mehr Informationen und unseren Shop finden Sie unter www.first-security.com.

Fragen?

Unsere Experten stehen Ihnen gerne unter sales@first-security.com zur Verfügung.

Über First Security Technology (FST)

2001 mit Sitz in Chur gegründet, ist die FST führender Hersteller von Schwachstellen Management Lösungen. Mit in der Schweiz entwickelten Lösungen unterstützt die FST Unternehmungen dabei, IT Systeme durch Inventarisierung zu identifizieren, Schwachstellen in ihrer IT-Infrastruktur frühzeitig zu erkennen und durch geeignete Prozesse die Risiken zu minimieren. Die IT-Sicherheit wird gewährleistet, die Effizienz und Effektivität von IT-Systemen werden verbessert.

Weitere Informationen: <https://www.first-security.com>



swiss made
software