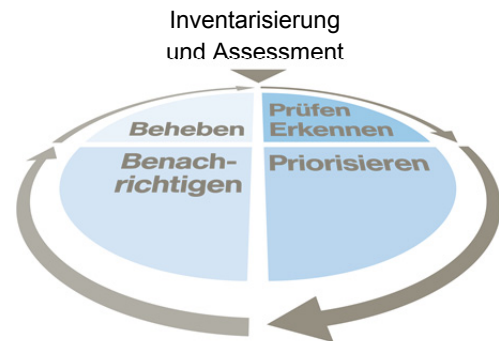


VulnWatcher – Swiss made Vulnerability Management (VM)

Was ist Vulnerability Management (VM)

Vulnerability Management (kurz VM; auf deutsch Schwachstellen Management) ist ein zyklischer, sich stetig wiederholender Prozess, der zur Identifizierung, Klassifizierung und Behebung von Schwachstellen in der gesamten IT-Infrastruktur (Hardware und Software). VM hat die Verringerung der Anfälligkeit der IT Infrastruktur auf Angriffe von innen und aussen zum Ziel, bevor die Angriffe erfolgen.

Schwachstellen sind Sicherheitslücken, die durch fehlerhafte oder falsch konfigurierte Hardware, fehlerhaften Programmcode oder nicht aktualisierte Infrastrukturen bestehen und dadurch die Integrität von Computersystemen kompromittieren können.



Wie ist VulnWatcher Vulnerability Management einsetzbar

VulnWatcher ist eine proaktive Sicherheitsmassnahme und damit einer der wichtigsten Bausteine eines IT-Sicherheitskonzeptes. Im Gegensatz zu defensiven Sicherheitsmassnahmen wie IDS/IPS oder Antivirus-Programmen ermöglicht der Einsatz von VM, Sicherheitslücken zu schliessen, bevor diese ausgenutzt werden. Voraussetzung für den sinnvollen Einsatz von VM ist die regelmässige Prüfung einer IT Infrastruktur und die unmittelbare Behebung von angezeigten Schwachstellen.

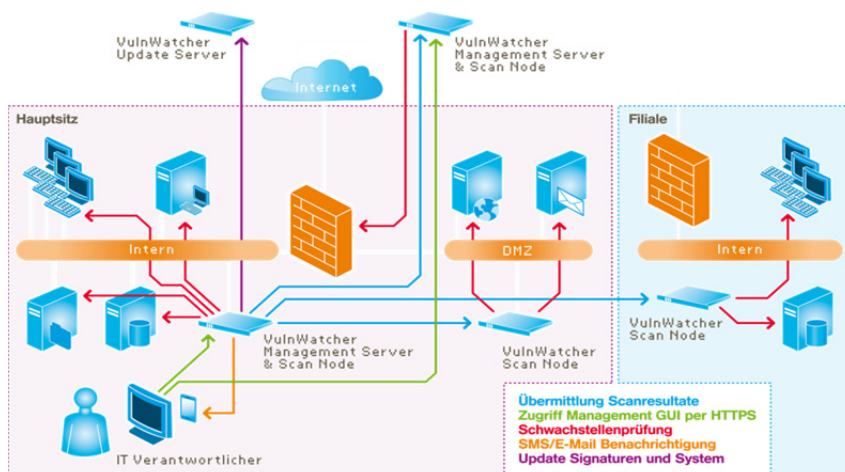
Wo wird VulnWatcher Vulnerability Management eingesetzt

VulnWatcher kann und sollte in jeder IT Infrastruktur regelmässig zum Einsatz kommen.

VulnWatcher ist unabhängig von jeglichen Betriebssystemvorgaben oder Technologien. VulnWatcher überprüft alle in der IT Infrastruktur integrierten Hardware-Komponenten sowie die installierte Software auf Schwachstellen.

VulnWatcher kann als Software-as-a-Service (SaaS) zur externen Prüfung der IT Infrastruktur eingesetzt werden. In diesem Fall ist keine zusätzliche Hard- oder Software in die IT Infrastruktur zu integrieren und zu betreiben. Die Überprüfung der IT Infrastruktur auf Schwachstellen kann jederzeit und unmittelbar vorgenommen werden.

VulnWatcher-on-an-Appliance wird vorwiegend zur internen Prüfung der IT Infrastruktur eingesetzt. Dazu wird zusätzliche Hard- und Software (eine sog. Appliance) in die zu überprüfende IT Infrastruktur integriert.



VulnWatcher-on-an-Appliance ermöglicht es, eine IT Infrastruktur von innen wie von aussen zu überprüfen und zu überwachen. Externe und interne Prüfung miteinander kombiniert ergeben zusammen einen umfassenden und zuverlässigen Schutz vor Schwachstellen.

Zudem kann VulnWatcher auch in einer virtualisierten Umgebung implementiert werden (VulnWatcher-on-Virtual-Machine).

Nutzen von VulnWatcher

- Erhöhung der Compliance & IT-Sicherheit durch regelmässige Schwachstellenüberwachung (proaktive Verifizierung, Bewertung und Behebung von Schwachstellen)
- Prozessoptimierung durch automatisierte Scans mit integrierter individuell definierbarer Risikobeurteilung, Alarmierung und Tracking-System
- Datenhaltung unternehmensintern oder in unserem VulnWatcher-Rechenzentrum in der Schweiz
- Integrierter Feed mit bis zu 45'000 IT-Schwachstellen
- Stufengerechtes Reporting bis hin zum IT-Revisionsbericht

VulnWatcher Versionen und Merkmale

	VulnWatcher Basic	VulnWatcher Prime
Scan extern/intern	Externe Scans	Externe und interne Scans
Anzahl Benutzer	Max. 5 Benutzer	unlimitiert
Lizenzmodell	IP basierend Max. 30 IPs	IP und Scan basierend Min. 5 IP oder 10 Scans
Mandantenfähigkeit	Ja	Ja
Reporting	Standard-Reports	Individuelle und Standard-Reports
Scan Engines	OpenVAS	OpenVAS und Nessus (optional)
VulnWatcher-on-an-Appliance	Nein	Ja
VulnWatcher-on-Virtual Machine	Nein	Ja
Schnittstellen zu externen Applikationen	Nein	Ja
Assessment	Top 1000 Ports Ohne Historie	Keine Limitierung Mit Historie
Web Application Scanning	Ja	Ja

Kernfunktionalität:

- Zentrale Administration
- Integriertes Ticket-System und Schnittstellen zu externen Ticket-Systemen (
- Einfaches, skalierbares Lizenzmodell
- Rollenbasierte Gruppenrichtlinien (ACL)
- Leistungsfähige Inventarisierung und Assessment der IT Infrastruktur (IPv4/IPv6)
- Zuverlässige Erkennung von Schwachstellen und Elimination von False Positives und False Negatives
- Standardisierte oder voll-individualisierte Risikoberechnung und Priorisierung
- Benachrichtigung von Personen und Gruppen per SMS und E-Mail gemäss individuell definierten Schwellenwerten
- Tägliche Aktualisierung der Schwachstellen-Datenbank
- VulnWatcher-on-an-Appliance voll skalierbar und clusterfähig
- Integriertes Backup
- Lifetime* Support für Appliance und Software (* lifetime: solange Appliance und Software genutzt werden)

Weitere Informationen:

Verkauf: sales@first-security.com
 Support: support@first-security.com
 Internet: <http://www.first-security.com>

Der Einsatz von VulnWatcher ermöglicht es unseren Kunden das Gefahrenpotential, welcher die IT Infrastruktur täglich ausgesetzt ist, besser zu erfassen, zu bewerten, zu bearbeiten und zu vermindern. VulnWatcher-as-a-Service prüft und überwacht den Perimeter der IT Infrastruktur vor unerlaubtem Zugriff von aussen. Mit VulnWatcher-on-an-Appliance und VulnWatcher-on-Virtual-Machine kann die IT Infrastruktur von aussen wie auch von innen überprüft und überwacht werden.

Referenzen:



Über First Security Technology (FST): Swiss Made Vulnerability Management!

FST mit Sitz in Chur ist der führende Hersteller von Schwachstellen-Assessment und –Management-Lösungen in der Schweiz. FST entwickelt Sicherheitslösungen als Software-as-a-Service, Virtual-Machine-basierend oder als Appliance und vertreibt diese über ein Netz von ausgewiesenen Händlern und Distributoren. FST's Sicherheitslösungen umfassen vollautomatische Schwachstellenerkennung, IT Infrastruktur-Assessment, Schwachstellenbeseitigung und –überwachung sowie IT Compliance erfüllende Reporting-Mechanismen.

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

