RiskWatch

itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 München

Tel.: +49 (0) 89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

www.itWatch.de
info@itWatch.de

RiskWatch - Ihr individuelles (Risiko-) Lagebild

Erstellung eines individuellen Lagebildes Ihrer IT und Erkennen der Risiken -Sicherheit im Unternehmen – In Echtzeit. Verarbeiten Sie die erkannten Risiken in der für Sie richtigen Geschwindigkeit.
RiskWatch ist eine selbstverbreitende Technologie zur automatischen Erfassung von IT-Risiken auf Microsoft Clients und Servern Sie ist CPU- und Daten-orientiert und nicht Netz-zentriert. Mit RiskWatch erstellen Sie ein individuelles Lagebild ihrer Cyber-Risiken im Unternehmen und erkennen folgende Szenarien:

- **Tatsächliche Angriffe auf die IT-Infrastruktur, die noch nicht bekannt sind**
- **Personalisierte Angriffe, zum Beispiel nach Social Engineering Attacken**
- **Advanced Persitant Threats**

Natürlich können Sie bei komplexen, mehrstufigen Angriffen und Bedrohungen mit der itWESS auch gleich erfolgreiche Schritte gegen die Angriffe unternehmen und die etwaig schon eingenisteten Malware-Komponenten sicher wieder entfernen.

RiskWatch – der einfach Start in die komplexe Welt der Cyber Security

IT-Sicherheitslösungen gibt es zu genüge, doch welche benötige ich wirklich? RiskWatch setzt den ersten Meilenstein, wenn Sie sich noch unklar sind in welche Technologien investiert werden soll. RiskWatch unterstützt den Experten, der schon viele IT-Sicherheitskomponenten im Einsatz hat, mit einfachen Übersichtsfunktionen. RiskWatch unterstützt dabei nicht nur die Forensik bei erkannten Bedrohungen oderAngriffen , RiskWatch ist auch ein Wegweiser, der bei der Dimensionierung von weiteren IT-Sicherheitslösungen unterstützt. So können damit konkrete Handlungsempfehlungen abgeleitet werden und die Projektierung von Cyber Security, Schutz vor Datendiebstahl (DLP) oder Advanced Persistend Threads (APT) und vielen weiteren Szenarien kann effizient gestaltet werden. Statistische Bewertungen der Verbesserungen durch Vorher/Nachher-Betrachtungen und der Verfolgung kritischer Werte (Security Score Card) werden offensichtlich.

Risiken erkennen und adäquat handeln

Die nötigen Sensoren für die Informationsbeschaffung für ein individuelles Lagebild werden mit RiskWatch bereitgestellt. Die dadurch erkannten Problemfelder lassen sich, wenn gewünscht, schnell und unkompliziert über die itWESS lösen ohne neue Installation. Zusätzlich können weitere Sensoren einfach und schnell integriert werden (z.B. mit PlugIN-Technik eigene Werkzeuge verwenden über offene Schnittstellen).

Einfache und kosteneffiziente Einbindung

Die Installation und Konfiguration von RiskWatch erfolgt über einen One-Click Install automatisch. Dafür ist kein spezielles Know-How erforderlich. Es gibt keine Performance-Einbußen beim Client und somit auch keine Beeinträchtigung der Produktivität des Nutzers. Es werden keine benutzerspezifischen Daten erfasst, so dass keine Überwachung der Benutzer durchgeführt wird.
Die Sichtung und Analyse der Daten erfolgt über Reports in einer Webanwendung, die keine Installation benötigt. Diese ist intuitiv und erfordert keine Schulung oder Berater. Zusätzlich ist die einfache Anbindung an Drittsysteme wie Reporting, SIEM, Forensik etc. möglich. Alle Reports können in standardisierten Austauschformaten exportiert werden.

Beispiele für Reports mit RiskWatch

Bei allen Reports können die allgemeinen Daten, wie der zu betrachtende Zeitraum und ähnliches, frei definiert werden.

Überblick über den Einsatz von angeschlossenen Peripherie-Geräten:

- USB-Laufwerke, USB-Geräte, FireWire, Bluetooth, tragbare Geräte (Handys etc.), Modems usw.
- Wann, wie lange, wie oft und bei Bedarf wo wurden Geräte angeschlossen
- Sortiert nach Typen und Häufigkeit des Anschlusses

Anmeldefehlversuche:

- Wann, wo, von wo und mit welcher Kennung ist eine Anmeldung in der IT-Infrastruktur des Unternehmens fehlgeschlagen
- Versuche einer parallelen Anmeldung
- Sortiert nach Häufigkeit pro Rechner und pro Kennung
- Ergänzend hier auch die Dauer der Anmeldung

Anwendung gestartet von externen Datenträgern

- Die am häufigsten von externen Datenträgern gestarteten Anwendungen
- Von welchem Datenträger (Seriennummer, Laufwerk, ProzessID, Größe) sind Anwendungen wann und auf welchem Rechner gestartet worden
- Erstellung einer Gesamtauflistung
- Sortiert nach Häufigkeit

Programmdateiveränderungen:

- Wie viele neue Programmdateien wurden erstellt
- Wie viele Programmdateien wurden verändert
- Welche wurde am häufigsten verändert oder neu erstellt
- Wann fand die letzte Veränderung der Programmdatei statt

Bedrohungen durch Malware:

- Übersicht über Dateien, die als potentiell gefährlich eingestuft werden

Eigene individualisierte Berichte:

- Eigene Zusammenstellung von protokollierten Sensordaten

Informationsabfluss auf mobile Datenträger:

- Wie viele Dateien sind mit welchem Volumen wann abgeflossen
- Auflistung pro Rechner (sortiert nach Anzahl)
- Anschließend Sortierung alphabetisch nach Dateityp
- Übersicht darüber wann und von welchem Rechner welche Datei auf welchen Stick (mit Hilfe der Seriennummer) übertragen wurde

FSRIW-190428