zubIT-SecurityScan

Sichern Sie Ihre Computer, Server & Webseiten

Jeden Tag werden neue Sicherheitslücken entdeckt. Sicherheitslücken sind für Ihre Infrastruktur, Ihre Daten und damit für Ihr Unternehmen eine ernsthafte Gefahr. Dies betrifft nicht nur die Hard- und Software, sondern kann im Ernstfall Ihr gesamtes Unternehmen mit Vertrieb, Produktion und Kommunikation stilllegen.

Dabei steht nicht nur Ihr Unternehmen auf dem Spiel, sondern auch Ihre Geschäftspartner und Kunden können in Mitleidenschaft gezogen werden. Mit diesen Gefahren sind alle Unternehmen konfrontiert – egal ob klein oder gross. Um sich und Ihr Unternehmen abzusichern, haben wir die Lösung:

zubIT-SecurityScan ist ein Security Information Management System (SIM). Damit überprüfen wir Ihre Infrastruktur und Ihre Website auf potentielle Sicherheitsrisiken, so dass diese dann abgestellt werden können. zubIT-SecurityScan stellt so die natürliche Evolution, in einer Zeit erhöhten IT-Sicherheitsrisikos, als notwendige Ergänzung zu Firewall und Anti-Virus Lösungen dar.

Vorteile auf einen Blick

- Erkennen Sie früh und schnell potentielle Sicherheitsrisiken
- Über 35.000 Prüfroutinen
- Aufspüren von Risiken in Ihrer Infrastruktur und Ihrer Webseite
- Mit unserer Expertise helfen wir Ihnen die Sicherheitslücken zu schließen
- Tägliche Aktualisierung der Prüfroutinen mit Unterstützung vom BSI und DFN

Systemumgebung

- Debian, Python, GIT
- Windows, Linux, Mac OS X, BSD, AIX, Solaris, HPUX
- Verfügbar als fertig konfigurierte Hardware oder als virtuelle Maschine

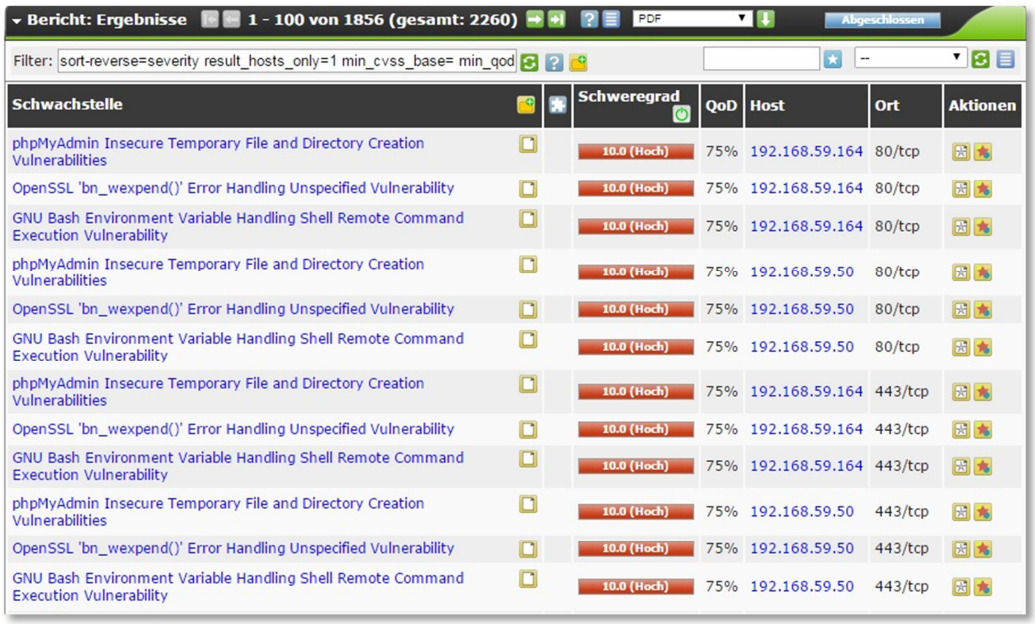
Umfangreiche Sicherheitsprüfung…

Um die Risiken aufzuspüren, wird Ihre Infrastruktur mit über 35.000 täglich aktualisierten Prüfroutinen und Ihre Website zusätzlich auf über 200 Sicherheitslücken getestet. Neue und alte Schwachstellen in der Software und Firmware Ihrer Geräte werden dabei genauso geprüft, wie schwache Passwörter für von außen erreichbare Systeme.

Wir prüfen auch Ihre internet-basierten Dienste auf Sicherheitslücken wie SQL-Injection, Cross-Site Scripting, leicht zu erratende Passwörter, nicht abgefangene Anwendungsfehler und Fehlkonfigurationen im IIS, Apache, PHP u.v.m. Optional können auch externe Webseiten geprüft werden.

Ausführliche Auswertung nach Risiko

Unsere Lösung zeigt Ihnen in kürzester Zeit den dringendsten Handlungsbedarf:



Bericht: Ergebnisse 1 - 100 von 1856 (gesamt: 2260) — Abgeschlossen

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod

Schwachstelle	Schweregrad	QoD	Host	Ort	Aktionen
phpMyAdmin Insecure Temporary File and Directory Creation Vulnerabilities	10.0 (Hoch)	75%	192.168.59.164	80/tcp	
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	75%	192.168.59.164	80/tcp	
GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability	10.0 (Hoch)	75%	192.168.59.164	80/tcp	
phpMyAdmin Insecure Temporary File and Directory Creation Vulnerabilities	10.0 (Hoch)	75%	192.168.59.50	80/tcp	
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	75%	192.168.59.50	80/tcp	
GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability	10.0 (Hoch)	75%	192.168.59.50	80/tcp	
phpMyAdmin Insecure Temporary File and Directory Creation Vulnerabilities	10.0 (Hoch)	75%	192.168.59.164	443/tcp	
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	75%	192.168.59.164	443/tcp	
GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability	10.0 (Hoch)	75%	192.168.59.164	443/tcp	
phpMyAdmin Insecure Temporary File and Directory Creation Vulnerabilities	10.0 (Hoch)	75%	192.168.59.50	443/tcp	
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	75%	192.168.59.50	443/tcp	
GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerability	10.0 (Hoch)	75%	192.168.59.50	443/tcp	

Ein Auszug einer Analyse – mehrere Funde mit dem höchsten Schweregrad

Ihre Sicherheit

- Über 7.900 neue Sicherheits-lücken allein 2014
- 1.914 kritische Sicherheitslücken 24% aller neu entdeckten Sicherheitslücken sind als kritisch eingestuft
- 2.751 mehr Lücken entdeckt als vor 18 Monaten
- 100% aller bisher durch den zubIT-SecurityScan getesteten Infrastrukturen offenbarten kritische Sicherheitslücken

weitere Informationen

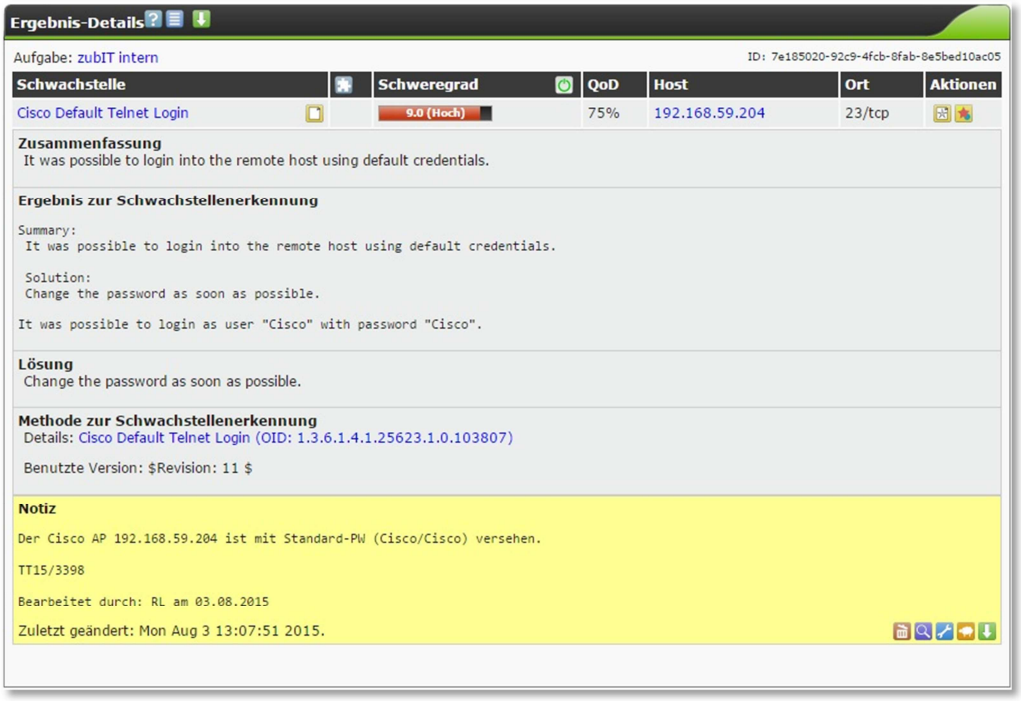
http://securityscan.zubit.de/

edv-anwendungsberatung
zühlke & bieker gmbh
beratung ● softwarelösungen ● systemintegration ● support

www.zubIT.de
martinistraße 11
45657 recklinghausen
tel 0 23 61 | 90 543-21
fax 0 23 61 | 90 543-22

Detaillierte Hinweise zur Bearbeitung

Auf diese Weise gewinnen Sie schnell und zuverlässig einen vollständigen Überblick möglicher Risiken und eine Handlungsempfehlung für jedes Event:



Häufige Gefahr – Router und Gateways werden mit Standard-Kennwörtern installiert

Bei der ausführlichen Analyse und Abschaltung dieser Sicherheitslücken können wir Ihnen mit unserer jahrelangen Erfahrung zur Seite stehen.

Flexible Lösungen

Unsere Lösung ist passend für Sie verfügbar:

- Als zubIT-Scanbox (Hardware Appliance mit vorkonfigurierter Software). Dies ist ein von uns vorbereiteter Micro Server, der einmalig oder dauerhaft in Ihre Infrastruktur integriert wird
- Als fertig eingerichtete virtuelle Maschine (VM)
- Als einmalige oder permanente Dienstleistung

Dabei begleiten wir Sie selbstverständlich Schritt für Schritt.

BSI und DFN unterstützte Prüfroutinen

Die von uns eingesetzte Software OpenVAS wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Deutschen Forschungsnetz (DFN) unterstützt. So sind Sie immer auf dem neusten Stand und können schnell auf neue Risiken reagieren.

Non-invasiver Scanvorgang

Der Prüfvorgang selbst beeinflusst den Betrieb nicht und Sie können normal weiter arbeiten. Ihre Infrastruktur und Webseiten bleiben unverändert.

Schnell und einfach – im Inneren wie im Äußeren: Ihren aktuellen Sicherheitsstatus gegenüber äußeren Gefahren ermitteln wir, ohne auf Ihrer Seite Einstellungen vornehmen zu müssen.