

**Your value added reseller:**

**QKomm GmbH**  
 In Gerderhahn 36a, 41812 Erkelenz, Germany  
 Tel.: +49 24 31/ 980 893, Fax: +49 24 31/ 980 894,  
 e-mail: office@qkomm.de, www.qkomm.de,  
 www.GDPdU-email.de , www.qcom-shop.de



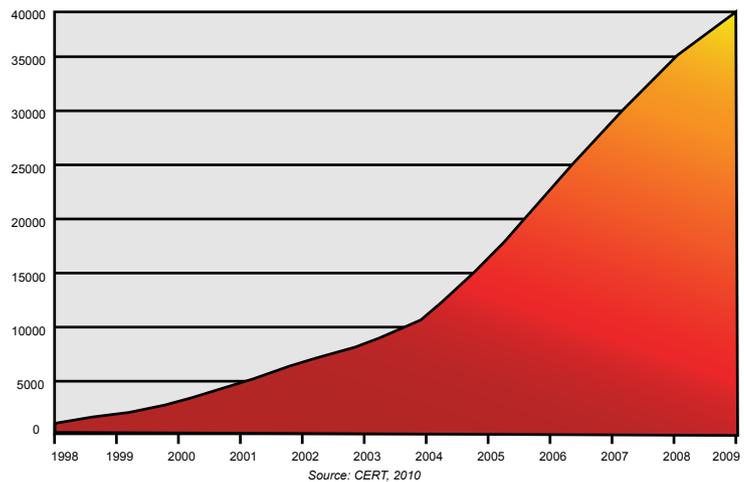
## Wie sicher ist Ihr Netzwerk? Überprüfen Sie es auf Schwachstellen!

Ohne Zweifel stellen Netzwerk Attacken eine zunehmende Bedrohung für Unternehmen aller Größen dar. Web Seiten werden gehackt und deren Inhalte verändert, Kundendaten und sensitive Personaldaten werden gestohlen, Sicherheitsvorfälle bedeuten Netzwerk- und Produktionsausfälle und intellektuelles Eigentum gerät durch Wirtschafts- und Industriespionage in die falschen Hände. Die Cyber-Kriminalität hat eine besonders beängstigende Entwicklung zu einem organisierten Wirtschaftszweig genommen, der mit gestohlenen Daten wie Kreditkarten Details und Passwörtern handelt und die dafür benötigten Werkzeuge über eine gut funktionierende Untergrundwirtschaft im Internet bezieht.

## Wie werden die Attacken durchgeführt?

Grundsätzlich gibt es nur zwei Möglichkeiten, in ein Netzwerk einzubrechen: entweder nutzt der Angreifer die Sicherheitslücken in Software und Hardware (Sicherheitsschwachstellen) oder er benutzt die fehlerhaften Konfigurationen von Geräten im Netzwerk (Konfigurationsschwachstellen).

Neue Schwachstellen werden heute in großer Zahl entdeckt und die Anzahl bekannter Schwachstellen beträgt jetzt mehr als 40.000\*. Die traditionellen reaktiven Abwehrmechanismen wie Firewalls, Anti-Viren Software und Intrusion Detection Systeme sind wichtige Bausteine der IT Sicherheit, bieten aber heute nicht mehr ausreichenden Schutz.



## Wie kann ich für Sicherheit in meinem Netzwerk sorgen?

Sofern Sie nicht bereits eine Schwachstellen Management Lösung in Ihrem Unternehmen implementiert haben ist der erste Schritt die Durchführung einer einmaligen Schwachstellen Überprüfung. Diese zeigt die Lücken in Ihrem Netzwerk an und bewertet das damit vorhandene Risiko. Als Ergebnis erhalten Sie Ihren aktuellen Sicherheitsstatus.

Outpost24 bietet Ihnen individuelle Netzwerk Schwachstellen Analysen, in denen unsere Sicherheitsexperten die Überprüfungen durchführen und Ihnen danach die Ergebnisse sowohl in Management Reports darstellen wie auch in detaillierten technischen Reports. Die Ergebnisse werden gemeinsam mit unseren Experten besprochen.

Für die Überprüfungen verwenden wir die führende Schwachstellen Analyse Technologie von Outpost24, und wir bieten diese Überprüfungen zu folgenden Preisen\*\* an.

Anzahl IP's	Preis
bis zu 5	€ 595
bis zu 10	€ 995
bis zu 50	€ 1995
bis zu 100	€ 2995
bis zu 250	€ 4995
bis zu 500	€ 7995

\*Nationale Schwachstellen Datenbank, <http://nvd.nist.gov/>

\*\*Diese Preise gelten nur für einmalige Überprüfungen. Reisekosten und Spesen können additiv anfallen.

# Outpost24: Schwachstellendiagnose und -behandlung in IT-Netzwerken

Outpost24 bietet einfache, schnell bereitzustellende und benutzerfreundliche Lösungen für die kontinuierliche Diagnose und Behandlung von Schwachstellen in Netzwerken.

Die Nutzung der speziellen Dienste entspricht dem Einsatz eines hoch qualifizierten Sicherheitsteams zum permanenten Aufspüren von Schwachstellen. Gefundene Schwachstellen werden bewertet und mit einer Behandlungsempfehlung in einem Bericht nach Gefährlichkeit zusammengefasst.

Die Ergebnisse können im Zeitablauf verglichen werden, um eine Trendaussage über das Gefährdungspotential abzuleiten.

Der Prozess der Behandlung von Schwachstellen wird durch eine Workflow Software unterstützt, welche die Delegation von Aufgaben an zuständige Administratoren erlaubt.

Im Gegensatz zur manuellen Schwachstellendiagnose kann eine automatisierte Diagnose viel häufiger durchgeführt werden. Dies ist deshalb wertvoll, weil neue Bedrohungen schon nach kurzer Zeit erkannt werden und das Risikopotential ansonsten mit der Zeit kontinuierlich ansteigen würde seit der letzten Diagnose. Hinzu kommen, dass rechtliche Anforderungen und die Notwendigkeit zur Einhaltung von Standards für IT Sicherheit weiterhin steigen.

## Outpost24 bietet folgende Lösungen für das IT Schwachstellen Management:

**OUTSCAN** ist eine SaaS-Lösung zur Diagnose von Schwachstellen, die aus dem Internet heraus genutzt werden kann. OUTSCAN untersucht die IPs im öffentlichen Netzwerk.

**HIAB** (Hacker In A Box) ist eine sofort nutzbare Webapplikation, die vorkonfiguriert auf einer netzwerkfähigen Hardware zur Diagnose von Sicherheitslücken innerhalb des Firmennetzwerkes ausgeliefert wird. Alle Daten werden auf der Appliance abgelegt und verlassen nie das Kundennetzwerk.

**Web Application Scanning** ist eine SaaS-Lösung zur Diagnose der Schwachstellen in Web Applikationen (auch speziell entwickelten) und Web Servern. Der Web Application Scanner kann alleine genutzt werden oder integriert in OUTSCAN und/ oder HIAB.

Untersucht werden Cross Site Scripting und SQL Injection Schwachstellen sowie virtuell gehostete Seiten. Außerdem können remote file include, command injection, code injection, format string issues, cross-site request forgery und CRLF injection aufgespürt werden.

## Outpost24: On-Demand PCI Compliance Prüfung

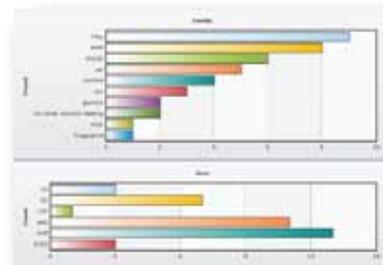
In den vergangenen Jahren haben Sicherheitsvorfälle mit Kreditkartendaten die Medien wachgerüttelt. Die betroffenen E-Commerce Betreiber, Retailer, Banken und Kreditkarteninstitute mussten in Gerichtsverfahren Stellung beziehen und verloren Image, Vertrauen und Geld.

Als Maßnahme gegen die kriminellen Machenschaften hat die Kreditkartenindustrie (inkl. American Express, Discover Financial Services, JCB, MasterCard Worldwide und Visa) den PCI Security Standards Council gegründet. Dieser Ausschuss hat den Payment Card Industry Data Security Standard (PCI DSS) entwickelt, einen umfassenden Sicherheitsstandard für das Arbeiten mit Kreditkartendaten.

Outpost24 ist ein vom PCI Security Standards Council zertifizierter Approved Scanning Vendor (ASV). Diese Zertifizierung ermöglicht es Outpost24 eine Lösung anzubieten, durch deren Einsatz Händler, Service Provider und Banken beweisen können, dass sie die Kreditkartendaten nach Vorgaben des PCI DSS bearbeiten und somit compliant sind.

**OUTSCAN PCI** ist das ideale SaaS-Werkzeug für Unternehmen aller Größen zur Erzielung der PCI DSS Compliance. OUTSCAN PCI bietet automatisiertes Netzwerkscannen, einfach zu interpretierende Berichte sowie Online Support zum Ausfüllen des PCI DSS Self-Assessment Questionnaire (SAQ).

\*\*The PCI Security Standards Council [Participating Organization/Approved Scanning Vendor/Qualified Security Assessor] logo is a trademark or service mark of The PCI Security Standards Council in the United States and in other countries.



**ÜBER OUTPOST24:** Outpost24 ist der Technologieführer in On-demand Schwachstellen Analyse und Management Lösungen. Wir sind unabhängig von allen Anbietern für Netzwerk Sicherheit und Infrastruktur. Unsere Lösungen sind weltweit bei mehr als 1.000 Unternehmen und Kunden der öffentlichen Hand im Einsatz. Outpost24 hat den Hauptsitz in Schweden und ist mit einem globalen Netzwerk lokaler Niederlassungen weltweit vertreten. Weitere Informationen zu Outpost24 finden Sie auf [www.outpost24.com](http://www.outpost24.com).