FORWARD THINKING IT SOLUTIONS

VULNERABILITY SCANS UND PEN TESTS FÜR PCI

Wie gut ist die IT-Infrastruktur gegen Angriffe von innen und aussen geschützt?

ergonomics

VULNERABILITY SCANS UND PEN TESTS FÜR PCI

Verifizieren Sie die Sicherheit Ihrer IT-Systeme gemäss den Vorgaben der Kartengeldindustrie

Daten von Kredit- und Debitkarten sind besonders kritisch, da ein Missbrauch umgehend direkten finanziellen Schaden verursachen kann. Deshalb haben die führenden Kreditkartenorganisationen mit dem Payment Card Industry Data Security Standard (PCI-DSS) einen weltweit gültigen Sicherheitsstandard etabliert. PCI-DSS wird vom PCI Security Standards Council (PCI SSC), einer Dachorganisation der Kreditkartenorganisationen Visa, MasterCard, Ampex und Discover, herausgegeben und administriert.

Unternehmen, die Zahlkartendaten verarbeiten, speichern oder übermitteln sind unter anderem verpflichtet, ihre IT-Systeme regelmässig mit einem PCI Security Scan auf Schwachstellen überprüfen zu lassen. Die Ergebnisse von solchen externen Scans werden nur dann anerkannt, wenn die Scans von einem zertifizierten Anbieter (Approved Scanning Vendor oder ASV) durchgeführt werden.

Vulnerability Scans

Unter einem Vulnerability Scan versteht man das Scannen eines Rechners oder einer Netzwerkkomponente mittels automatisierten Programmen und Tools. Der übliche Weg für einen automatisierten Vulnerability Scan ist das Starten eines oder mehrerer Tools, welche die Zielsysteme nach vordefinierten Sicherheitslücken abtasten. Die Liste der Sicherheitslücken muss laufend auf dem neuesten Stand gehalten werden. Externe Vulnerability Scans erfolgen direkt über das Internet, interne Scans werden im eigenen Netzwerk durchgeführt.

Vulnerability Scans laufen in der Regel automatisiert ab. Somit ist die Auswertung und Dokumentation der Resultate gemäss bestimmten Vorgaben (z.B. PCI ASV) möglich.

Pen Tests

Pen Tests (Penetration Tests) sind geplante, von einem autorisierten (White Hat) Angreifer durchgeführte Angriffe auf IT-Systeme. Der Angreifer versucht, mit Hilfe von Werkzeugen Schwachstellen zu finden oder beim Scan identifizierte Schwachstellen auszunützen.

Warum Ergonomics?

Ergonomics ist seit 2011 der Schweizer Dienstleister für alle Aufgabenstellungen rund um PCI-DSS. Für Vulnerability Scans und Penetration Tests arbeiten wir mit entsprechend spezialisierten Unternehmen zusammen. Unsere PCI-Spezialisten bieten Beratungs- und Auditdienstleistungen für das Erreichen der PCI-DSS Compliance. Somit ist die Ergonomics ihr einziger Ansprechpartner für alle PCI-DSS Belange.

Ein echter Penetrationstest beinhaltet manuelle Vorbereitung in Form der Sichtung des Prüflings, Planung der Testverfahren (black, grey oder white Box) und Ziele, Auswahl der notwendigen Werkzeuge und schliesslich die Durchführung und Dokumentation. Das Vorgehen und die allfälligen Erfolge eines Pen Tests hängen im Wesentlichen von der Erfahrung und der Kreativität des Angreifenden ab.

Ziele eines Penetrationstests sind

- Die Identifikation von Schwachstellen
- Das Aufdecken potenzieller Fehler, die sich aus einer fehlerhaften Bedienung oder Konfiguration ergeben können
- Die Erhöhung der Sicherheit auf technischer und organisatorischer Ebene
- Eine punktuelle Überprüfung von IT-Sicherheitsmerkmalen durch einen unabhängigen Dritten.

Kritisch ist bei Pen Tests die ausführliche Dokumentation von gewähltem Vorgehen, eingesetzten Tools und gewonnenen Erkenntnissen.

VULNERABILITY SCANS UND PEN TESTS FÜR PCI

PCI-DSS Vorgaben

Um die Anforderungen des PCI-DSS Standards erfüllen zu können, sind mindestens externe Vulnerability Scans erforderlich. Je nach Grösse und Ausprägung des Unternehmens können auch interne Vulnerability Scans sowie interne und externe Penetration Tests gefordert sein.

Die Vorgaben von PCI 4.0 erfordern, dass Pen Tests gemäss einem etablierten Verfahren durchgeführt werden.

Die für die PCI-DSS Compliance notwendigen externen Vulnerability Scans müssen zwingend von einem Approved Scanning Vendor (ASV) durchgeführt werden. So ist sichergestellt, dass die Tests gemäss den PCI-Vorgaben durchgeführt werden und dass die Dokumentation den Anforderungen des Standards entspricht.

Was kennzeichnet unsere externen PCI-DSS Security Scan Dienstleistungen aus?

- Mit einem normierten, international an erkannten Verfahren werden die aus dem Internet erreichbaren IT-Systeme (Server, Netzwerkkomponenten, Webserver und Webshops, etc.). auf viele tausend bekannte und ständig aktualisierte Schwachstellen über- prüft.
- Die externen PCI-DSS Security Scans werden für den öffentlichen IP Adressbereich des Unternehmens durchgeführt. Erkannte Schwachstellen werden nicht ausgenutzt. Eine Gefährdung des ordnungsgemässen Betriebs der IT-Systeme ist praktisch ausgeschlossen.
- Auf Wunsch führen wir die Scans für Ihr Unternehmen durch, präsentieren Ihnen die Resultate und die allenfalls notwendigen Massnahmen.
- Sie erhalten das Scanergebnis in Form einer Zusammenfassung und eines umfassenden technischen Berichts. Dieser enthält alle gefundenen Schwachstellen sowie detaillierte Vorschläge zu deren Behebung.
- Unsere Angebote beinhalten in der Regel eine unbegrenzte Anzahl Scans. So können Sie die Systeme häufig prüfen. Ob die festgestellten Schwachstellen erfolgreich behoben wurden, kann so umgehend nachgeprüft werden.
- Werden keine nach PCI-DSS kritischen Schwachstellen gefunden, ist Ihre IT Infrastruktur PCI-DSS konform und Sie erhalten einen Nachweis für Ihren Acquirer.
- Bei Fragen oder offenen Punkten unterstützen Sie unsere Experten.
- Aufgrund der ausserordentlich dynamischen Bedrohungslage sollten PCI-DSS Security Scans regelmässig durchgeführt werden. Wir empfehlen, gemäss PCI-Vorgaben, mindestens einmal im Quartal und nach relevanten Systemanpassungen zu scannen.

Ergonomics arbeitet bei externen PCI-Scans mit anerkannten Approved Scanning Vendors (ASVs) zusammen und kann so ein umfassendes Paket für PCI-DSS und weitergehende Sicherheitsanforderungen anbieten.

Die Ergonomics ist vom PCI Security Standards Council als QSA-Unternehmung zertifiziert. Unsere Spezialisten stehen für ein unverbindliches Gespräch gerne zur Verfügung.

VULNERABILITY SCANS UND PEN TESTS FÜR PCI

FORWARD THINKING IT SOLUTIONS

Die Ergonomics AG mit Hauptsitz in Zürich und einer Niederlassung in Bern wurde 1991 von den heutigen Inhabern gegründet. Das IT-Unternehmen mit gegen 25 Mitarbeitenden hat es sich von Anfang an zum Ziel gesetzt, auch den höchsten Ansprüchen zu genügen, die man an einen Partner stellen kann. Kompetenz, Erfahrung, Innovation und verantwortliches Handeln bilden das Fundament, auf dem wir als Unternehmen stets gebaut haben – der Erfolg hat uns Recht gegeben.

Ergonomics als führendes Beratungsunternehmen im Bereich der integralen Sicherheit unterstützt Sie, wenn es darum geht, unternehmensweite IT-Risiken, Gefahren und Schwachstellen zu erkennen und zu beheben.

Weitere Informationen finden Sie unter:
www.ergonomics.ch

Ergonomics AG >> Uetlibergstrasse 132 >> CH-8045 Zürich
+41 58 311 10 00 >> info@ergonomics.ch >> www.ergonomics.ch