Datenblatt
Vulnerability Scan (Schwachstellen Scan)
Technischer Sicherheitscheck

Die Grundlage für einen Angriff besteht typischerweise zu mehr als 70 Prozent aus der Sammlung von Daten. In dieser Phase wird das Angriffsziel definiert und Schwachstellen ausfindig gemacht, welche zu einem erfolgreichen Angriff führen. Für die Angreifer stehen die Mitarbeiter und Einzelarbeitsplätze genauso im Visier wie computergesteuerte Maschinen oder komplexe Netzwerke. Um sinnvolle Maßnahmen gegen interne und externe Angriffe zu ergreifen, ist eine detaillierte Schwachstellenanalyse aller Komponenten notwendig. So identifizieren Sie Schwachstellen bevor Angreifer es tun.

Externer Schwachstellen Scan

Unsere Sicherheitsexperten analysieren ihre Systeme von außen nach bekannten Schwachstellen. Auch Firewall-Systeme befinden sich im Fokus der Angreifer. Durch die Fehlkonfiguration von Firewall Systemen können Hacker das Intranet kompromittieren. Neue Angriffsszenarien wie z.B. History Stealing von Intranet Webseiten aus den Browsercache eines Benutzers versetzen Angreifer in die Lage, Struktur-Informationen des Intranet zu extrahieren. Des Weiteren können sogar Port Scans durch ausgeklügelten JavaScript-Code über den Browser des Clients im Intranet durchgeführt werden. Deswegen ist die Aktualität und Funktionalität von Firewall-Systemen und Deep-Packet-Inspection Systemen umso wichtiger. Unsere Experten analysieren die Ergebnisse des Schwachstellen Scans und entwickeln Härtungsmaßnahmen um Angriffen vorzubeugen. Mit dem Schwachstellen Scan wird Angriffen aus dem Internet auf Webservices, Webseiten insbesondere mittels Top-10 Schwachstellen (nach OWASP), z.B. Cross-Site Scripting, HTML Injection oder Browserstring Injection, effektiv entgegen gewirkt.

Interner Schwachstellen Scan

Je größer die Organisation umso komplexer ist das interne Netz und desto größer ist die Wahrscheinlichkeit eines erfolgreichen Angriffs aus dem eigenen Netz. Die eigenen Mitarbeiter oder externe Mitarbeiter mit Zugang zum internen Netz können (un)wissentlich Schadsoftware einschleusen. Sind die Angreifer einmal im Netz können die einzelnen Sicherheitszonen, z.B. Firewall-Systeme kompromittiert werden. Dadurch erweitert sich der Raum eines Angreifers. Im Falle eines erfolgreichen Angriffs von innen oder außen sind somit die wichtigsten Werte eines Unternehmens, z.B. Produktions- oder Kundendaten, gefährdet. Heutzutage ist Cyberkriminalität weit verbreitet und Wirtschaftsspionage mit diesen Techniken eine gängige Methode.

Vulnerability Scan Report

Die aus dem Schwachstellen-Scan gewonnenen Informationen erhalten Sie in Form eines Schwachstellen-Berichts (Vulnerability Scan Report). Dieser beinhaltet Empfehlungen für die Stärkung der Sicherheit Ihrer IT-Infrastruktur. Unsere Security-Experten analysieren die Ergebnisse des Vulnerability Scans anhand von Best Practices und geben wertvolle Hinweise zur Optimierung der IT-Sicherheit - um internen und externen Angriffen vorzugreifen.

Wussten Sie schon,...

... dass seit der Einführung der EU Datenschutzgrundverordnung IT-Dienstleister (z.B. Rechenzentren) für Informationssicherheit und Datenschutz eigenverantwortlich sind?

... dass der finanzielle Schaden eines erfolgreichen Angriffs im Schnitt 2,4 Mio. € beträgt? (PwC , Information Security Survey 2015)

... dass 2015 über 439 Mio. Windows-Schadsoftwarevarianten erkannt wurden? (Bericht zur Lage der IT-Sicherheit in Deutschland 2015)

... dass 1/3 der Unternehmen in den ersten 6 Monaten 2016 durch Ransomware (z.B. Locky) betroffen waren? (Umfrage zur Betroffenheit durch Ransomware – 04/2016, Allianz für Cyber-Security)

Unsere Leistung auf einen Blick.

Der Vulnerability Scan erfolgt zum Festpreis, standardisiert in vier Phasen:

- Phase 1: Vorbereitungsgespräch bei Ihnen vor Ort
- Phase 2: Durchführung des Schwachstellen-Scan auf ausgewählten Systemen
- Phase 3: Analyse und Auswertung
- Phase 4: Ergebnispräsentation bei Ihnen vor Ort

Im Vorbereitungsgespräch identifiziert unser Expertenteam Ihre individuellen IT-Sicherheitsanforderungen. Der Scope des Scans wird entsprechend Ihrer Bedürfnisse definiert und festgelegt. Nachdem die Beauftragung stattgefunden hat, starten unsere IT-Security-Experten den Schwachstellen Scan. Dabei werden die Systeme nach bekannten Schwachstellen überprüft. Der gesamte Scan wird von unseren Experten jederzeit überwacht. Nach Beendigung des Schwachstellen-Scans werden die Ergebnisse in einem detaillierten Bericht zusammengestellt und die Empfehlungen zur Behebung der Sicherheitslücken aufgelistet. In der Abschlusspräsentation stellt das Expertenteam die Ergebnisse der Analyse und die daraus resultierenden Handlungsempfehlungen vor. Die Durchführungsdauer beträgt drei Tage.

Der Mehrwert.

Unser Expertenteam ermittelt und erkennt interne und externe Schwachstellen in Ihren Systemen. Sie erhalten Handlungsempfehlungen, um Ihre Organisation und Systeme vor potenziellen Angriffsvektoren zu schützen. Die Spezialisten von Fujitsu entdecken für Angreifer ausnutzbare, lückenhafte Konfigurationen in Netzwerk- und Serversystemen. Ihre Systeme werden durch das Scannen Systeme nach fehlenden Patches vor Zero-Day Attacken abgehärtet. Sie erhalten einen detaillierten Report über die erkannten Angriffsvektoren und begleiten Sie bei der Evaluation des Berichts. Folgende Leistungen sind enthalten:

- Suche nach bekannten Schwachstellen
- Analyse unter Berücksichtigung aktueller Exploits
- Einstufung der Kritikalität der Schwachstellen nach CVSS (Common Vulnerability Scoring System)
- Scan im Hintergrund
- Empfehlung von konkreten Maßnahmen zur Härtung Ihrer Infrastruktur
- Managementgerechte Aufbereitung und Darstellung der Ergebnisse

Servicedetails

Detaillierte Leistungsbeschreibung

- **Phase 1: Vorbereitungsgespräch bei Ihnen vor Ort**
  - Definition & Dokumentation der Projektziele (Scope)
  - Vorstellung und Abstimmung des Projektablaufs mit Festlegung von Zeitplänen

- **Phase 2: Durchführung des Schwachstellen-Scans**
  - Tool-gestützter Scan durch unsere Security-Experten
  - Angepasst auf die mit Ihnen individuell definierten Ziele

- **Phase 3: Analyse und Auswertung der Befunde**
  - Zusammenführen und Aufbereitung der Ergebnisse
  - Entwicklung von Handlungsempfehlungen zur Härtung

- **Phase 4: Ergebnispräsentation bei Ihnen vor Ort**
  - Managementgerechte Präsentation
  - Übergabe der ermittelten Ergebnisse

Lieferumfang

Power Point Präsentation: Analyse der Befunde

- Überblick über gefundene Schwachstellen und resultierende Gefährdungen
- Managementgerechte Beurteilung der Befunde
- Handlungsempfehlungen für Härtungsmaßnahmen

Bericht: Analyse der gefundenen Schwachstellen

- Auflistung aller gefundenen Schwachstellen
- Einstufung der Kritikalität jeder Schwachstelle

Ihre Beistellungsleistung

Beistellungsleistung Ihrerseits sind:

- Teilnahme der Verantwortlichen für Ihren IT-Betrieb und IT-Sicherheit am Vorbereitungsgespräch (0,5 Tag).
- Bei internen Scans Netzwerk-Einstellungen (Firewall- und Portfreigaben) und ein Benutzerkonto mit ausreichenden Berechtigungen für die Dauer des Scans
- Teilnahme der Verantwortlichen für Ihren IT-Betrieb und IT-Sicherheit an der Abschlusspräsentation (0,5 Tag).
- Ansprechpartner für den Zeitraum der Maßnahme

Geschäftsbedingungen

Sofern nicht ausdrücklich anders vereinbart, werden die IT-Serviceleistungen der Fujitsu gem. dieses Datenblattes auf Basis der *„Allgemeinen Geschäfts Bedingungen für Lieferungen und Leistungen der Fujitsu"* insbesondere dem Teil E *„Weitere Dienst- und Werkleistungen"* erbracht.

Bestellung und Lieferung

Der *Vulnerability Scan (Schwachstellen Scan)* kann von dem vertrieblichen Ansprechpartners Ihres Vertrauens bezogen werden.
Folgende Angaben sind in Ihrem Auftrag erforderlich:

Titel	**Vulnerability Scan (Schwachstellen Scan)**
Bestellnummer	**CPS:SC-SSP-00006VD**

Weitere Informationen

Fujitsu Portfolio

Zusätzlich zu diesem Consulting Service bietet Fujitsu eine Vielzahl an weiteren Services, aber auch Plattformlösungen. Diese kombinieren leistungsstarke Produkte von Fujitsu mit optimalen Servicekonzepten, langjähriger Erfahrung und weltweiten Partnerschaften.

Dynamic Infrastructures
Mit seiner Fujitsu Dynamic Infrastructures-Strategie bietet das Unternehmen ein vollständiges Portfolio an IT-Produkten, -Lösungen und -Services – von Client- und Rechenzentrumslösungen sowie Managed Infrastructures bis hin zu Infrastructure-as- a-Service. Wie groß der Nutzen der Technologien und Services von Fujitsu ist, hängt von dem von Ihnen gewählten Maß der Kooperation ab. Damit erreicht Ihre IT die nächste Ebene in Bezug auf Flexibilität und Effizienz.

Computing-Produkte
www.fujitsu.com/de/products
- PRIMERGY: Industriestandardserver
- SPARC Enterprise: UNIX-Server
- BS2000/OSD Mainframes
- PRIMEQUEST: geschäftskritischer IA-Server
- ETERNUS: Speicherlösungen
- ESPRIMO, LIFEBOOK: Arbeitsplatzsysteme

Software
www.fujitsu.com/de/products/software
- Betriebssysteme
- Middleware
- Anwendungen
- Partner-Software

Services
www.fujitsu.com/de/services
- Business Application Services
- Data Center Services
- End User Services
- Security Services
- Compliance & Manufacturing Services

Weitere Informationen

Um mehr über Fujitsu Security Services oder andere Services zu erfahren, wenden Sie sich bitte an Ihren Fujitsu-Vertriebsmitarbeiter oder schreiben Sie eine E-Mail an Einfach.Sicher@ts.fujitsu.com
oder besuchen Sie unsere Website unter www.fujitsu.com/de/security-services

Fujitsu Green Policy Innovation

Fujitsu Green Policy Innovation ist unser weltweites Projekt zur Reduzierung der Umweltbelastung. Mithilfe unseres globalen Know-hows streben wir eine Lösung der Probleme hinsichtlich umweltfreundlicher Energienutzung über die IT an. Weitere Informationen finden Sie unter:
www.fujitsu.com/global/about/environment

Copyright

© Copyright: 2017 Fujitsu Technology Solutions GmbH
Fujitsu, das Fujitsu-Logo und Fujitsu-Markennamen sind Marken oder eingetragene Marken von Fujitsu Limited in Japan und anderen Ländern. Andere Firmen-, Produkt- und Servicebezeichnungen können Marken oder eingetragene Marken der jeweiligen Eigentümer sein.

Haftungsausschluss

Änderungen bei den technischen Daten vorbehalten. Lieferung unter dem Vorbehalt der Verfügbarkeit. Haftung oder Garantie für Vollständigkeit, Aktualität und Richtigkeit der angegebenen Daten und Abbildungen ausgeschlossen. Wiedergegebene Bezeichnungen können Marken und/oder Urheberrechte sein, deren Benutzung durch Dritte für eigene Zwecke die Rechte der Inhaber verletzen kann.

Kontakt

FUJITSU
Enterprise & Cyber Security
Consulting & Professional Services
E-Mail: Einfach.Sicher@ts.fujitsu.com

Postanschrift:
Mies-van-der-Rohe Str. 8, 80807 München
Telefon: +49 (0) 89 / 62060 - 0
Webseite: www.fujitsu.com/de