Schneider + Wulf

Cloud + Infrastruktur
Digitalisierung
Sicherheit

360° IT Service

Pentest Schwachstellenanalyse Schwachstellen-Management Social Engineering

IT-Sicherheits-Dienstleistungen von Schneider + Wulf

Whitepaper

Inhalt

Disclaimer

Unsere Angebote, bereitgestellte Dokumente sowie Mitteilungen sind ausschließlich für Sie bestimmt und müssen vertraulich behandelt werden. Die Weitergabe sowie Vervielfältigung unserer Unterlagen sowie die Verwertung und Mitteilung ihres Inhaltes an Dritte ist nicht gestattet, soweit dieses von uns nicht schriftlich freigegeben worden ist. Zuwiderhandlungen verpflichten zu Schadensersatz.

01 | Penetrationstest

Durch einen Penetrationstest kann geprüft werden, inwieweit die Sicherheit der IT-Systeme durch Bedrohungen von Hackern gefährdet ist und ob die IT-Sicherheit durch die eingesetzten Sicherheitsmaßnahmen aktuell gewährleistet wird. Gelingt dem Penetrationstester der Einbruch in Teile der Computer-Systeme und ist er in der Lage, an vertrauliche Informationen zu gelangen oder diese zu manipulieren, ist dies der Beweis für eine Sicherheitslücke.

Beim **Penetrationstest** handelt es sich um zielgerichtete Angriffe gegen Computer-Systeme. Ziel soll es sein, auch in abgesicherten IT-Infrastrukturen Schwachstellen zu identifizieren und auszunutzen. Ein Penetrationstest sollte nur dann durchgeführt werden, wenn im Vorfeld durch eine **Schwachstellenanalyse** die offensichtlichen Sicherheitsprobleme bereits identifiziert und behoben wurden.

Ein Penetrationstest ist zudem immer nur eine Momentaufnahme der IT-Sicherheitslage, deshalb sollte die IT-Infrastruktur regelmäßigen Überprüfungen unterzogen werden. So ist es beispielsweise möglich, dass nach Abschluss des Penetrationstests durch eine menschliche Fehlentscheidung oder durch Installation einer Software ein neues gravierendes Sicherheitsproblem entsteht.

Bezüglich der Qualität der als Penetrationstest bezeichneten Dienstleistung existieren große Unterschiede. Das Niveau und der praktische Nutzen eines Penetrationstests wird im Wesentlichen davon bestimmt, inwieweit auf die individuelle Situation des Auftraggebers eingegangen, wie viel Zeit und Ressourcen auf die Ausforschung von Schwachstellen verwendet und wie kreativ dabei vorgegangen wird.

Die Ziele eines Penetrationstest sind unter anderem folgende:

- Erhöhung der Sicherheit Ihrer technischen Systeme
- Identifikation von nicht offensichtlichen Schwachstellen
- Bestätigung der IT-Sicherheit durch einen externen Dritten
- Erhöhung der Sicherheit Ihrer organisatorischen und personellen Infrastruktur

Module

Für Penetrationstests bieten wir die folgenden Module an, die unabhängig voneinander buchbar sind. Nachfolgend finden Sie ein paar Beispiele für mögliche Testszenarien. Das genaue Testszenario erarbeiten wir mit Ihnen in einem persönlichen Gespräch. Darauf aufbauend erstellen wir für Sie das finale Angebot.

P | INTERNET

Wir prüfen Ihre über das Internet erreichbaren Systeme. Dies kann beispielsweise das VPN Gateway, der Citrix oder Mail Server sein. Wir prüfen die exponierten Dienste dabei auf Schwachstellen und versuchen, uns nach Möglichkeit Zugriff auf einen der Server zu verschaffen und uns von dort aus weiter in das interne Netzwerk zu arbeiten.

P | LAN

Im Modul P-LAN werden vornehmlich die internen Netzwerk-Strukturen geprüft. Wie ist Ihre Switch-Infrastruktur abgesichert? Setzen Sie verwundbare Protokolle ein? Gibt es Möglichkeiten, aus einem entsprechenden VLAN auszubrechen? Etc. Wir bieten Ihnen zudem an, die Sicherheit Ihrer bereits eingesetzten Schutzmechanismen wie Intrusion Prevention oder Network Access Control-Systeme zu überprüfen.

P | RADIO

Hierbei prüfen wir Ihre funkbasierten Dienste wie WLAN oder Bluetooth-Systeme. Ist das WLAN-Besuchernetz ordnungsgemäß vom produktiven Netz getrennt oder gibt es Schwachstellen in der Verschlüsselung oder Authentifizierung?

P | WEBSERVICE

Im Modul P-WEBSERVICE wird eine Web-Anwendung auf Schwachstellen wie SQL Injection, Local/Remote File Inclusion oder Cross-Site Scripting hin überprüft. Wir arbeiten dabei die vollständige Liste der OWASP TOP 10 ab. Eine Web-Anwendung kann dabei der von Ihnen betriebene Online Shop oder die Corporate Website sein.

P | APPLICATION

Bestandteil des P-APPLICATION-Moduls kann eine für sich eigenständige Anwendung wie Ihr ERP-System oder eine Individual-Entwicklung sein. Ein möglicher Testgegenstand wäre das Prüfen auf eine Rechteausweitung. Besteht zum Beispiel die Möglichkeit, Daten in einer Anwendung zu manipulieren oder zu stehlen? Des Weiteren prüfen wir Anwendungen auch auf Programmierfehler wie Stack und Heap Overflows.

P | SOCIAL

Durch einen Social Engineering-Test kann das Sicherheitsbewusstsein Ihrer Mitarbeiter geprüft werden. Wir unterscheiden dabei zwischen Human based und Computer based. Ein möglicher Ansatz wäre, durch fingierte Telefonanrufe an vertrauliche Informationen zu gelangen oder durch gezielte

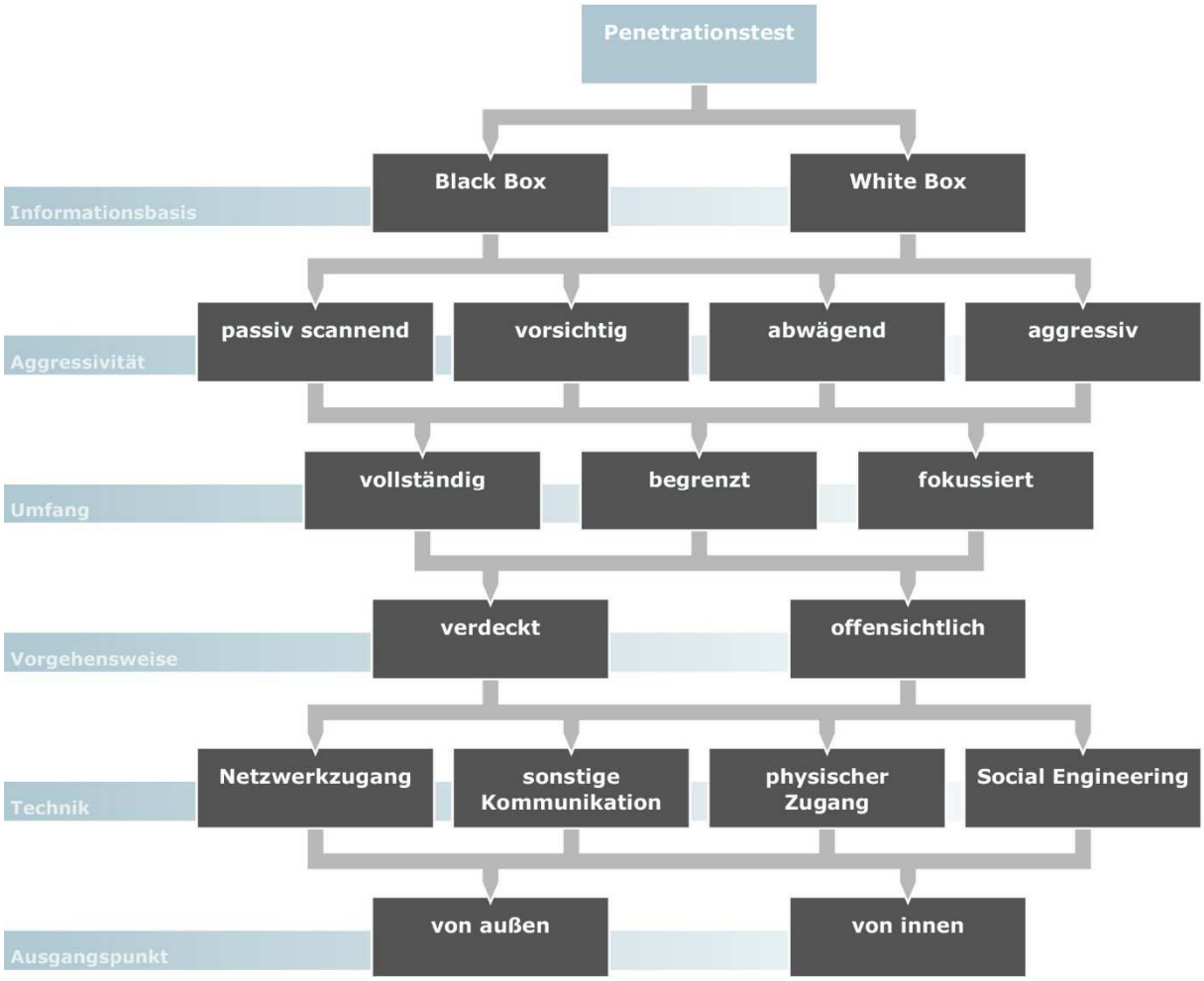
Phishing-Attacken ‚Spähprogramme' auf den Ziel-Systemen zu platzieren. Der Datenschutz spielt dabei für uns eine sehr große Rolle - jegliche personenbezogenen Daten werden nach Abschluss der Tests vollständig gelöscht. Heutige professionelle Angriffe beinhalten in den meisten Fällen immer auch eine Social Engineering-Attacke. Ein Angreifer wird immer den Weg des geringsten Widerstandes gehen. Sind Ihre Systeme sehr gut abgesichert, versucht ein Angreifer im zweiten Schritt, sich Zugriff durch Mitarbeiter Ihres Hauses zu verschaffen. Aus diesem Grund sind die Sensibilisierung und der regelmäßige Test heutzutage ein wichtiger Aspekt.

P | RETEST

Ein Retest sollte immer Bestandteil eines Penetrationstests sein. Durch den Retest wird geprüft, ob tatsächlich alle im Vorfeld aufgedeckten Schwachstellen ordnungsgemäß geschlossen wurden.

Klassifikation

Anhand der abgebildeten sechs Kriterien wird ein Penetrationstest typischerweise geplant, das erste Kriterium ist die **Informationsbasis**, diese sagt aus, nach welchem Modell vorgegangen wird und welche Informationen vom Kunden bereitgestellt werden. Die **Aggressivität** legt fest, mit welcher Intensivität ein Test durchgeführt wird, in hochkritischen Umgebungen empfiehlt sich eine abwägend/vorsichtige Herangehensweise.



Quelle | Bundesamt für Sicherheit in der Informationstechnik (BSI)

Eine **denkbare Klassifikation** würde zum Beispiel wie folgt aussehen:

Black Box | abwägend | fokussiert | offensichtlich | Netzwerkzugang | von außen

5-Phasen-Modell

Ein Penetrationstest gliedert sich üblicherweise in 5 Phasen, diese lauten wie folgt:

Vorbereitungsphase

In der Vorbereitungsphase werden gemeinsam mit dem Kunden die exakten Ziele des Penetrationstests besprochen, wie beispielsweise der Umfang, die Informationsbasis und die Aggressivität des Tests. Während eines Tests kann es in seltenen Fällen zu Ausfällen von Diensten kommen (Denial of Service). So ist es beispielsweise möglich, dass durch die automatisierten Tests vereinzelt Dienste abstürzen. Dies geschieht in der Regel bei extrem veralteter oder schlecht programmierter Software. Aus diesem Grund bieten wir dem Kunden auch eine Durchführung außerhalb der normalen Arbeitszeiten an. Zudem ist es möglich, die kritischen Systeme während der normalen Testzeiten außen vor zu lassen und diese zu einem geeigneteren Zeitpunkt zu prüfen.

Informationsbeschaffungsphase

Im Vorfeld wird mit dem Kunden besprochen, ob ein sogenannter Blackbox- oder Whitebox-Test durchgeführt werden soll. Bei einem Blackbox-Test werden kundenseitig lediglich die Ziele wie IP-Adressen und Host-Namen mitgeteilt und ein Netz-Zugang bereitgestellt. Entscheidet sich der Kunde für einen Whitebox-Test, erhalten wir detaillierte Informationen über das Ziel. Diese umfassen üblicherweise die eingesetzten Software-Produkte und Versionen der Systeme sowie Informationen über das zugrundeliegende Netzwerk. Anschließend kann mit der eigentlichen Informationsbeschaffung begonnen werden. Ziel ist es, eine möglichst komplette und detaillierte Übersicht über die installierten Systeme inklusive der potenziellen Angriffspunkte beziehungsweise der bekannten Sicherheitsmängel zu erlangen.

Bewertungsphase

Die in der Informationsbeschaffungsphase gewonnenen Informationen werden nun auf potenzielle Gefährdungen hin geprüft. Die daraus resultierenden Gefährdungen fließen im Anschluss in die Phase ‚Aktive Eindringungsversuche' ein.

Aktive Eindringungsversuche

Hierbei werden aktive Versuche unternommen, in die zuvor ausgewählten Systeme einzudringen, da diese Phase von allen anderen die Risikoreichste ist, wird dieser Schritt ausschließlich manuell und mit großer Sorgfalt durchgeführt.

Abschlussanalyse und Berichtsphase

In dieser Phase wird ein detaillierter Bericht mit allen gefundenen Sicherheitsmängeln erstellt. Jeder Sicherheitsmangel wird einzeln bewertet und der Kunde erhält Vorschläge zu Maßnahmen, wie die jeweiligen Mängel behoben werden können.

In einem gemeinsamen Abschlussgespräch besprechen wir den aus dem Penetrationstest resultierenden Bericht und die sich daraus ergebenden Maßnahmen.

02 | Schwachstellenanalyse

Die **Schwachstellenanalyse**, auch oft als ‚Vulnerability Assessment' bezeichnet, hat zum Ziel, eine möglichst vollständige Liste aller Sicherheitsprobleme in Ihrem Unternehmen aufzustellen. Meistens ist es so, dass der Kunde sich darüber bewusst ist, dass Sicherheitsprobleme in seiner Infrastruktur bestehen. Die Schwachstellenanalyse ist dabei das richtige Werkzeug, um diese Probleme zu identifizieren und zu priorisieren.

Eine Schwachstellenanalyse ist immer nur eine Momentaufnahme der IT-Sicherheitslage. Deshalb sollte die IT-Infrastruktur regelmäßigen Überprüfungen unterzogen werden. So ist es beispielsweise möglich, dass nach Abschluss der Schwachstellenanalyse durch eine menschliche Fehlentscheidung oder durch Installation einer Software ein neues gravierendes Sicherheitsproblem entsteht.

Während einer Schwachstellenanalyse wird mit Hilfe von automatisierten und manuellen Überprüfungen nach Schwachstellen gesucht. Die automatisierten Scans geben im ersten Schritt einen guten Überblick über die verwundbaren Systeme. Die Ergebnisse müssen jedoch auf sogenannte ‚false positives' hin geprüft werden. Aus diesem Grund führen wir eine Reihe manueller Überprüfungen durch, um die Testergebnisse zu verifizieren und Falschmeldungen auszuschließen. Nach Abschluss der Tests erhalten Sie einen Report mit allen gefundenen Sicherheitsproblemen. Wir geben Ihnen dabei zu jedem Sicherheitsproblem einen Vorschlag mit, wie das Problem gelöst werden kann. Auf Wunsch unterstützen wir Sie auch technisch bei der Fehlerbehebung.

Die Ziele einer Schwachstellenanalyse sind unter anderem folgende:

- Erhöhung der Sicherheit Ihrer technischen Systeme
- Identifikation von Schwachstellen
- Bestätigung der IT-Sicherheit durch einen externen Dritten
- Erhöhung der Sicherheit Ihrer organisatorischen und personellen Infrastruktur

Module

Für eine Schwachstellenanalyse bieten wir die folgenden Module an, die unabhängig voneinander buchbar sind. Um einen vollständigen Überblick über das Sicherheitsniveau eines Unternehmens zu erhalten empfehlen wir, interne und externe Systeme zu überprüfen.

S | INTERNET

Wir führen einen vollständigen Scan Ihrer über das Internet exponierten Systeme durch. Anschließend werden die gesammelten Ergebnisse bewertet und gegebenenfalls weitere manuelle Überprüfungen durchgeführt.

S | LAN

Wir führen einen vollständigen Scan Ihrer im internen Netzwerk befindlichen Systeme durch. Wie im Modul S-INTERNET werden hierbei ebenfalls alle Ergebnisse bewertet und gegebenenfalls weiteren Überprüfungen unterzogen.

S | RETEST

Ein Retest sollte immer Bestandteil einer Schwachstellenanalyse sein. Durch den Retest wird geprüft, ob tatsächlich alle im Vorfeld aufgedeckten Schwachstellen ordnungsgemäß geschlossen wurden.

03 | Schwachstellen-Management

Kontinuität ist im Bereich der IT-Sicherheit ein maßgeblicher Punkt, der heute noch zu sehr unterschätzt wird. IT-Systeme sollten durch ein stetiges Monitoring auf neue oder veränderte Schwachstellen geprüft werden. Mit dem **Schwachstellen-Management** bieten wir eine Dienstleistung an, die genau dieses Problem löst.

Mit Hilfe professioneller Software überwachen wir Ihre, über das Internet erreichbaren oder im internen Netzwerk befindlichen Systeme und alarmieren Sie bei einer potenziellen Bedrohung. Diese kontinuierliche Überprüfung auf Schwachstellen ist nicht mit einer Intrusion Prevention-Lösung zu vergleichen, denn wir sind damit im Stande, sogenannte ‚Credentialed Checks' durchzuführen. Dabei meldet sich die Monitoring Software über Protokolle wie SSH, SMB oder WMI mit einem priviligierten Benutzer am zu überprüfenden System an und kann somit auch Fehler in internen Konfigurationen aufdecken und alarmieren.

Für über das Internet erreichbare Systeme kann das Monitoring durch unsere Server durchgeführt werden. Für eine Überprüfung interner Systeme wird eine kleine Appliance, welche wahlweise als Hardware oder VM erhältlich ist, in Ihrem Netzwerk installiert und meldet etwaig auftretende Vorkommnisse an eine von uns bereitgestellte, zentrale Instanz.

Selbstverständlich bieten wir dem Kunden einen dedizierten Account und umfangreiche Auswertungsmöglichkeiten an, um die Ergebnisse selbst prüfen zu können.

Firmenprofil Schneider & Wulf EDV-Beratung

Messbar herausragender Service seit 1988 - störungsfreie und leistungsstarke IT-Lösungen. Jährlich erarbeiten wir in mehr als 300 Kundenprojekten und weit über 5.000 Supports für aktuell 1.700 KMU mit 20 bis 250 PC-Arbeitsplätzen zukunftssichere IT-Infrastrukturen, die einfach funktionieren.

Mit Standorten in Frankfurt am Main und im hessischen Babenhausen operieren wir im Rhein-Main-Gebiet, aber auch deutschland- und europaweit am Markt.

Unsere Erfahrung spiegelt sich in unserer Ausrichtung wieder: Wir sind immer für unsere Kunden da - so unbürokratisch wie möglich, dabei jedoch immer aufmerksam, strukturiert und absolut professionell - bei 100%iger Kostentransparenz.

Um störungsfreie und leistungsstarke IT-Lösungen zu gewährleisten, arbeiten wir präventiv statt reaktiv. Das bedeutet: Wir vermeiden und beheben Störungen, bevor sie zum Problem werden.

Adressiert werden inhabergeführte KMU, deren Entscheider verstanden haben, dass IT kein notwendiges Übel, sondern ein wichtiger Baustein erfolgreicher Unternehmensplanung ist.

Kontakt

Schneider & Wulf EDV-Beratung GmbH & Co KG
Im Riemen 17 | 64832 Babenhausen
www.schneider-wulf.de | info@schneider-wulf.de
Fon +49 6073 6001-0 | Fax +49 6073 6001-99