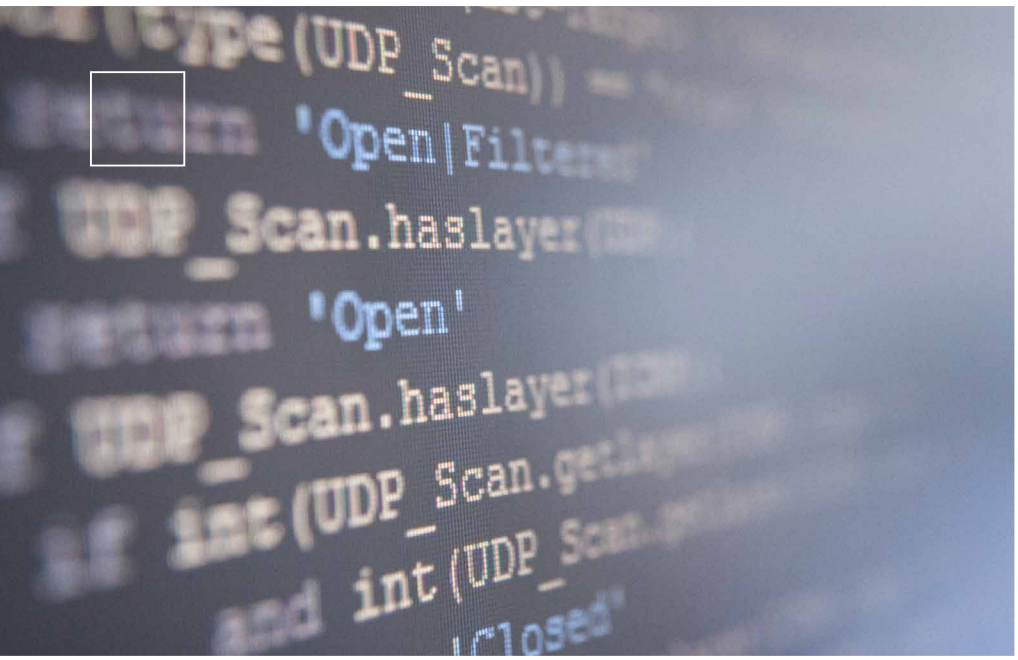
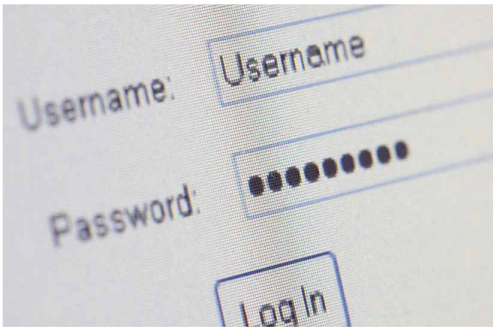




Praktizierte Informationssicherheit

Penetrationstests

datenschutz nord GRUPPE

Inhalt

VORWORT

Zunehmende Attacken aus dem Internet haben in den letzten Jahren das Thema Informationssicherheit für Unternehmen unverzichtbar gemacht. Dennoch führen unzureichend administrierte Server, veraltete Software oder Programmierfehler immer wieder zu erfolgreichen Angriffen u.a. auf E-Mail und Webserver, aber auch auf Industrieanlagen (Industrie 4.0).

Um Ihr Unternehmen zuverlässig vor missbräuchlichen Internetattacken und den damit oftmals verbundenen wirtschaftlichen Schäden und Imageverlusten zu schützen, ist es nicht nur wichtig, im Unternehmen ein so genanntes Informationssicherheits-Management (ISMS) aufzubauen, das Sicherheitsrisiken frühzeitig identifiziert sowie Verbesserungsvorschläge formuliert und entsprechende Maßnahmen umsetzt. Zu dem Thema ISO 27001 und zertifizierte Informationssicherheit hatten wir bereits eine Broschüre herausgegeben.

Vielmehr ist es – ergänzend zum Aufbau eines ISMS – auch notwendig, die Risikoanalyse durch gezielte Penetrationstests zu ergänzen. Erst durch reale Tests, in denen konkret versucht wird, missbräuchlich Zugriffsrechte auf Servern zu erhalten, können belastbare Aussagen über die Qualität der umgesetzten IT-Sicherheitsmaßnahmen getroffen werden.

In der vorliegenden Broschüre geben wir Ihnen einen Überblick über unsere Vorgehensweise bei der Durchführung von Penetrationstests. Welche Tests für Ihr Unternehmen am geeignetsten sind, entnehmen Sie unseren Testmodulen, die je nach Prüfschwerpunkt auch kombiniert werden können. Auf diese Weise können wir Ihnen einen maßgeschneiderten Penetrationstest anbieten.

Nehmen Sie gern Kontakt zu uns auf! Wir sind beim BSI als IT-Sicherheitsdienstleister für Penetrationstests zertifiziert,

Ihr Team der datenschutz nord Gruppe

1.
IT-Sicherheit und Penetrationstests

Um das Sicherheitsniveau Ihrer Systeme festzustellen, Schwachstellen und Sicherheitslücken zu identifizieren sowie potentiellen Angriffen am effektivsten vorzubeugen, empfiehlt sich die Durchführung von gezielten und individuellen Penetrationstests. Bei einem Penetrationstest simulieren wir einen kontrollierten Angriff und geben dabei Antworten auf folgende wichtige Fragen:

- Können externe Angreifer die Firewall umgehen?
- Können Externe aufgrund veralteter Softwareversionen die Kontrolle über E-Mail- oder Web-Server übernehmen?
- Können sich Unbefugte über einen Exploit Zugriff auf sensible Daten verschaffen?
- Können Kundendaten aus einer Webapplikation mittels SQL-Injection oder Cross-Site-Scripting ausgelesen werden?
- Können Geräte oder Industrieanlagen manipuliert werden, so dass diese nicht mehr funktionieren oder sogar eine Gefahr darstellen?

Mit unserer umfangreichen Expertise und langjährigen Erfahrung im Bereich der Penetrationstests können wir Ihre IT-Sicherheit zuverlässig prüfen und verbessern. Sofern wir Sicherheitslücken oder Verbesserungspotentiale erkennen, schätzen wir zum einen das mögliche Schadenspotential ein und geben Ihnen zum anderen entsprechende Handlungsempfehlungen.

Ein Penetrationstest hat, abhängig von der Prüftiefe und der Größe des Untersuchungsgegenstandes, in vielen Fällen einen stichprobenartigen Charakter. Eine absolute Sicherheit kann damit nicht garantiert werden. Unser

Ziel ist es daher, durch regelmäßige Penetrationstests das aktuelle Sicherheitsniveau anzuheben, so dass erfolgreiche Cyber-Angriffe gegen Ihr Unternehmen sehr unwahrscheinlich sind.

Wir sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als eines von wenigen Unternehmen als IT-Sicherheitsdienstleister für Penetrationstests zertifiziert. Wir setzen ausschließlich BSI-zertifizierte Penetrationstester ein, deren fachliche Qualifikation durch das BSI geprüft wurde.

Beispiel 1:
Attacken auf KMUs

Auch kleine und mittelständische Unternehmen verwenden für viele Aufgaben Webanwendungen: Content-Management Systeme, Online-Shops oder spezielle Kundenportale werden dazu genutzt, um das Unternehmen im Internet zu präsentieren; häufig werden hierüber sensible Kunden- und Zahlungsdaten verarbeitet. Auch firmenintern werden in der Personal- oder Projektverwaltung Webanwendungen eingesetzt, da hierzu nur ein Browser benötigt wird.

Bei der Entwicklung, Installation und Konfiguration solcher Webanwendungen tauchen immer wieder Schwachstellen auf, die Angreifer für ihre Zwecke missbrauchen. So war es beispielsweise in einer populären E-Commerce-Lösung möglich, durch eine ungenügende Validierung von Parametern per SQL-Injection Datenbanken von Online-Shops auszulesen und auf sensible Kundendaten zuzugreifen.

Um einem solchen Szenario vorzubeugen, suchen wir in einem Penetrationstest gezielt nach derartigen Schwachstellen. Per Portscan werden zunächst die Dienste und das Betriebssystem des Servers festgestellt. Anschließend wird die Webanwendung auf potentielle Schwachstellen (siehe Kapitel 4.2 Modul Webapplikationen) getestet.

Beispiel 2:
Attacken auf industrielle Anlagen

Wie das BSI vor einiger Zeit berichtete, wurden die Industrieanlagen eines deutschen Stahlwerks über das Netz attackiert. Angriffe auf Industrieanlagen sind besonders kritisch, da durch Manipulation industrieller Prozesse nicht nur wirtschaftlicher Schaden durch Produktionsausfall oder Gerätedefekt entstehen kann. Je nach Art und Konfiguration der Anlagen kann ein Angriff auch Personen- und Umweltschäden durch einen Industrieunfall verursachen.

Im Falle eines Stahlwerks haben sich die Angreifer vom Büronetz des Unternehmens bis zu den Steuerungscomputern vorgearbeitet. Über gezielt auf das Unternehmen angepasste Phishing-Attacken wurden Bürocomputer per E-Mail mit Schadsoftware infiziert, um hierüber zunächst die interne Netzstruktur des Stahlwerks auszuforschen. Anschließend gelangten die Angreifer offenbar an Steuerungscomputer für Hochöfen, so dass es möglich war, die Steuerung dieser Anlagen zu manipulieren und die Anlagen teilweise sogar vollständig abzuschalten. Hauptursache einer derart folgenschweren Hackerattacke war die fehlende Trennung zwischen hochkritischen Produktivsystemen und dem Kommunikations- und Datennetz des Unternehmens.

In einem differenzierten Penetrationstest prüfen wir sowohl externe als auch interne Systeme gezielt unter folgender Fragestellung: Ist es einem Angreifer möglich, von außen erreichbare Systeme wie z.B. einen Web- oder E-Mailserver anzugreifen, um darüber in das interne Unternehmensnetz zu gelangen? Welche Zugriffsmöglichkeiten bestehen im Erfolgsfall im internen Netz? Ist das Unternehmen gegenüber Phishing- und Social Engineering Attacken verwundbar?

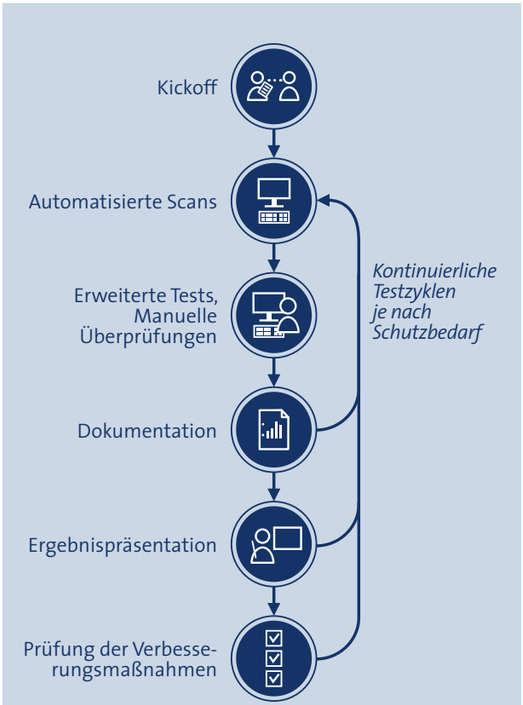
2.
Vorgehensmodell

Zu jedem Penetrationstest gehören eine umfassende Vor- und Nachbereitung. Dabei werden die Ziele des Tests mit Ihnen definiert und mögliche Risiken für die Systeme geklärt. Bei der Durchführung von vollständigen Penetrationstests kommt der Vermeidung von ungewollten Betriebsstörungen eine hohe Bedeutung zu. Angriffe zur Blockierung eines Dienstes – sogenannte Denial-of-Service-Angriffe – werden grundsätzlich nicht durchgeführt.

Die Art und Gestaltung der Tests sind dabei von den jeweiligen Testmodulen, der gewählten Prüftiefe und Ausgangssituation sowie von den bis dato erzielten Prüfergebnissen abhängig. Dokumentiert werden nicht nur die gefundenen Schwachstellen, soweit wie möglich unterbreiten wir auch detaillierte Verbesserungsvorschläge.

Sofern die Penetrationstests regelmäßig durchgeführt werden sollen, um auch sicherheitsrelevante Systemänderungen zu evaluieren, vereinbaren wir mit Ihnen kontinuierliche Testzyklen. Je nach Höhe des Schutzbedarfs und Größe des Untersuchungsgegenstandes empfehlen wir eine quartalsweise, halbjährliche oder jährliche Wiederholung der Tests. Da bei jeder Änderung der IT-Infrastruktur neue Angriffsvektoren entstehen können und ggf. neue Sicherheitslücken und Gefährdungen seit dem Zeitpunkt des letzten Penetrationstest zu beachten sind, werden in der Regel alle Prüfungen vollständig wiederholt. Zudem werden die Schwachstellen des vorangegangen Tests bzw. die entsprechenden Verbesserungsmaßnahmen im Rahmen eines Delta-Tests erneut validiert. Aufgrund von Synergien bei der Testvorbereitung, der Scan-Auswertung sowie der Dokumentation können wir den Aufwand bei der erneuten Durchführung eines Penetrationstest entsprechend reduzieren und Ihnen damit bereits den ersten Testdurchlauf innerhalb des Gesamtpakets kostengünstiger anbieten. Je höher die Testfrequenz ist, desto mehr können Kosten in diesem Zusammenhang eingespart werden.

Typischerweise gliedert sich ein Projekt in folgende Meilensteine:



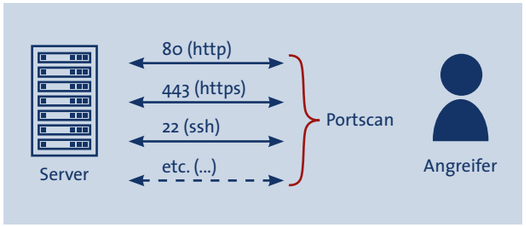
Kickoff

In einem Vorgespräch besprechen wir mit Ihnen zusammen die optimale Vorgehensweise für den von Ihnen gewählten Untersuchungsgegenstand und stellen die für Sie passenden Testmodule und Prüfthemen zusammen (siehe Kapitel 4). Ebenso wird festgelegt, welche Informationen wir vorab über den Prüfgegenstand vom Auftraggeber erhalten und ob der Test als Black-Box-, White-Box- oder so genannter Grey-Box-Test durchgeführt werden soll (siehe Kapitel 3). Schließlich werden die Ansprechpartner festgelegt.

Sofern Sie ein speziell auf Ihre Bedürfnisse angepasstes Sondermodul (siehe Kapitel 4.5) beauftragen möchten, kann das Vorgespräch weiterhin um ein Risk-Assessment ergänzt werden. Bei dieser vereinfachten IT-Risikoanalyse werden in einem ein- bis zweitägigen Workshop sämtliche sicherheitsrelevante Anwendungen und Schnittstellen Ihres Unternehmens gemeinsam erörtert, analysiert und bewertet. Die Ergebnisse des Workshops werden – ergänzt um evtl. vorhandene Unternehmensdokumente und -unterlagen zur IT-Sicherheit – ausgewertet, dokumentiert und zusammen mit Ihnen priorisiert. Im Anschluss daran können konkrete Anwendungen respektive Systeme, für die ein Risiko identifiziert wurde, mit Hilfe eines Penetrationstests näher untersucht werden.

Automatisierte Scans

In der Regel startet ein Penetrationstest mit der Durchführung von automatisierten Scans mittels speziell dafür angepasster Software. Dabei setzen wir sowohl auf kommerzielle Programme als auch auf selbst entwickelte Skripte und Tools. Während der Überprüfung eines Netzwerkes werden dabei zum Beispiel die extern und intern verfügbaren Dienste auf den Zielsystemen mit einem Portscan ermittelt (siehe Kapitel 4.1 Modul Netzwerke).



Dazu werden Verbindungen zu den entsprechenden Systemen aufgebaut, Anfragen gesendet und die Antworten ausgewertet. Je nach Ausgangssituation können dabei gesamte IP-Adressbereiche gescannt werden, wobei wir die relevanten Systeme im Rahmen eines Black-Box-Tests selbst ermitteln. Weiterhin können wir uns auf bestimmte IP-Adressen bzw. Systeme konzentrieren und die notwendigen Scan-Parameter an Ihre individuellen Netzwerkbedürfnisse anpassen. Um mögliche Intrusion Detection/Prevention Systeme (IDS/IPS) zu umgehen, können alle Tests sequentiell und mit einer entsprechenden Verzögerung durchgeführt werden.

Die ermittelten Dienste werden als Grundlage für einen passiven Schwachstellenscan genutzt. Ein passiver Schwachstellenscan zeigt mögliche Gefährdungen der Zielsysteme auf, wobei jedoch eventuell vorhandene Schwachstellen nicht aktiv überprüft und ausgenutzt werden. Es erfolgt lediglich ein Vergleich von Versionsnummern und System-Signaturen.

Beim automatisierten Scan einer Webapplikation erfolgt – nach einem Port- und Schwachstellenscan des zugrunde liegenden Webservers – weiterhin eine Überprüfung der Anwendung durch einen speziellen Webapplikationsscanner. Dabei werden funktionale Sicherheitslücken, welche sich unter anderem in Cross-Site-Scripting- und SQL-Injection-Schwachstellen widerspiegeln können, zuverlässig erkannt.

Sofern sich der Penetrationstest auf automatische Scans beschränkt (Produkt Security Scan), werden Ihnen die generierten Reports unserer Scan-Tools zur Verfügung gestellt.

Erweiterte Tests, manuelle Überprüfungen

Aufbauend auf den automatisierten Scans werden erweiterte Tests durchgeführt und die Ergebnisse manuell überprüft. Dabei werden die automatisierten Scans analysiert und validiert, um zum einen sogenannte False Positives auszuschließen und zum anderen potentielle Angriffsmöglichkeiten zuverlässig herauszufiltern.

Je nach Prüfgegenstand werden hierbei verschiedene Prüfaspekte evaluiert, die von uns speziell an den jeweiligen Untersuchungsgegenstand angepasst werden. Im Rahmen der manuellen Prüfungen werden auch konzeptionelle Schwachstellen sowie logische Fehler in den Abläufen der eingesetzten Software getestet, um zum Beispiel Sicherheitslücken innerhalb der Authentisierung und des Session-Managements einer Webanwendung aufzudecken. Sofern ein internes Netzwerk überprüft wird, werden weiterhin lokale Authentisierungsmechanismen getestet.

Auf Ihren Wunsch können wir im Kontext von sogenannten Post-Exploitation-Angriffen untersuchen, wie weit ein potentieller Angreifer durch das Ausnutzen einer Sicherheitslücke in Ihr Unternehmensnetzwerk vordringen könnte und welcher Zugriff auf vertrauenswürdige und sensible Daten dabei möglich wäre. Dadurch kann zum einen das konkrete Schadenspotential einer Schwachstelle besser beurteilt werden, und zum anderen nimmt der Penetrationstest eher den Charakter eines realen Angriffs an.

Um auch den sozialen Aspekt im Rahmen des Penetrationstests zu betrachten, kann zudem der Grad der Sensibilität Ihrer Mitarbeiter mit Hilfe von Social-Engineering-Methoden, wie zum Beispiel Phishing-Angriffen überprüft werden. Phishing-Angriffe können auch separat beauftragt werden.

Auswertung und Dokumentation

Nach der Durchführung aller Tests werden die Ergebnisse der automatisierten Scans sowie der manuellen Prüfungen ausgewertet und in verständlicher Form detailliert dokumentiert. Die Schwachstellen werden entsprechend ihrer möglichen Auswirkungen klassifiziert und es werden Empfehlungen zur Verbesserung der IT-Sicherheit gegeben.

Ergebnispräsentation

Auf Wunsch werden die Ergebnisse des Penetrationstests in einem gemeinsamen Termin präsentiert, wobei die aufgezeigten Schwachstellen näher erörtert werden. Die Präsentation kann dabei sowohl bei Ihnen als auch in unseren Räumlichkeiten stattfinden. In letzterem Fall besteht zusätzlich die Möglichkeit, bestimmte Schwachstellen sowie Angriffe in einer kurzen Live-Hacking-Demonstration vorzuführen.

Prüfung der Verbesserungsmaßnahmen

Sofern Sie keine vollständige Wiederholung des gesamten Penetrationstests benötigen oder längere Testzyklen wünschen, besteht die Möglichkeit, dass die umgesetzten Maßnahmen zur Beseitigung der Schwachstellen zu einem späteren Zeitpunkt nochmals überprüft werden. Die Ergebnisse werden wiederum in verständlicher Weise dokumentiert, ggf. werden weitere Empfehlungen ausgesprochen.

3.

Testszenarien

Grundsätzlich unterscheiden wir zwischen drei verschiedenen Testszenarien: Black-Box, White-Box und Grey-Box.

Black-Box Bei einem Black-Box-Test besitzen wir ausschließlich die benötigten Informationen, um den jeweiligen Untersuchungsgegenstand eingrenzen zu können, wie zum Beispiel den zu testenden IP-Adressbereich. Weitere Informationen über die zugrunde liegende IT-Infrastruktur stehen uns nicht zur Verfügung, so dass der Test einem realen, externen Angriff sehr nahe kommt.

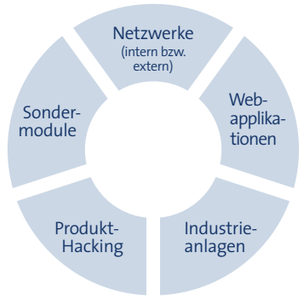
White-Box Im Rahmen eines White-Box-Tests stellen Sie uns umfangreiche Informationen über den Prüfgegenstand zur Verfügung. Dabei kann es sich sowohl um konkrete Netzwerkpläne als auch um Quellcode einer Anwendung handeln – also Informationen, die einem externen Angreifer in der Regel nicht zur Verfügung stehen, die aber bei ausreichender Zeit erraten werden könnten. Ein White-Box-Test ist vor allem dann sinnvoll, wenn der Schutzbedarf des Prüfgegenstandes hoch ist und ein entsprechender Angriff eher unwahrscheinlich ist.

Grey-Box Der Grey-Box-Test ist unser bevorzugter Ansatz bei der Durchführung eines Penetrationstests. Hierbei wird zunächst von einer Black-Box ausgegangen, wobei schrittweise wichtige Informationen für einen effektiven Test vom Auftraggeber preisgegeben werden. Dabei kann es sich beispielsweise um Anmeldedaten für eine Webapplikation handeln, um die Anwendung auch aus dem privilegierten Benutzerbereich qualifiziert testen zu können. Dieser Ansatz wahrt zum einen die notwendige Objektivität für ein realistisches Angriffsszenario und erlaubt zum anderen umfassendere Tests gegenüber dem Prüfgegenstand im Vergleich zu einem reinen Black-Box-Test.

4.

Testmodule und Prüfthemen

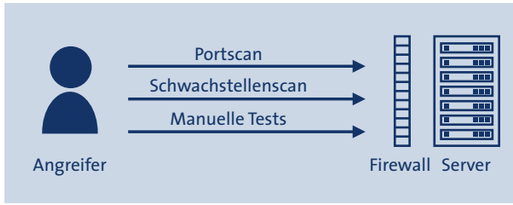
Passend zu Ihrem Prüfgegenstand können Sie zwischen fünf verschiedenen Testmodulen wählen bzw. diese kombinieren.



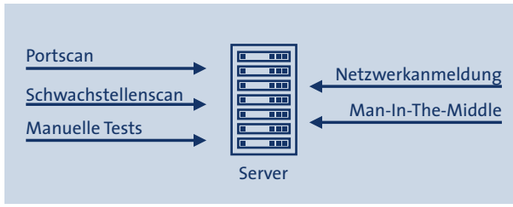
4.1

Modul Netzwerke

Sobald ein System aus dem Internet erreichbar ist, erfolgt nach durchschnittlich sieben Sekunden der erste Angriff durch automatisierte Programme, welche das Internet zu jeder Zeit und ohne Pause nach verwundbaren Zielen durchsuchen. Sofern sich Ihr Netzwerk als angreifbar herausstellt, werden mit großer Wahrscheinlichkeit zunächst ebenfalls automatisierte Attacken folgen. Falls sich Ihr Unternehmen weiterhin als lohnenswertes Angriffsziel herausstellt, besteht zudem die Gefahr von weitaus gefährlicheren und ausgefeilteren Angriffen durch erfahrene Hacker. Das Netzwerk-Modul unterscheidet deshalb zwischen internen und externen Netzwerken.



Von außen testen wir Ihre extern bzw. öffentlich erreichbaren Systeme, wie beispielsweise Web- oder E-Mail-Server, sowie komplette demilitarisierte Zonen. Dabei erfolgt indirekt auch eine Prüfung der entsprechenden Firewall-Regeln, indem ein Angriff aus dem Internet simuliert wird. Im Rahmen eines Black-Box-Tests untersuchen wir Ihren gesamten IP-Adressbereich und alle verfügbaren TCP- und UDP-Ports im Hinblick auf erreichbare Systeme und Netzwerkdienste.



Innerhalb Ihres Unternehmens testen wir nach dem Innentäter-Szenario Ihr Intranet auf mögliche Angriffsvektoren, wobei wir bei Bedarf auch entsprechende interne Firewall-Beschränkungen respektive VLAN-Konfigurationen überprüfen.

Aufbauend auf den automatisierten Port- und Schwachstellenscans untersuchen wir im Rahmen der manuellen Tests zahlreiche Themenbereiche, auf die wir im Folgenden ausführlicher eingehen.

Einsatz veralteter Software

Sowohl die installierten Dienste als auch das zugrundeliegende Betriebssystem eines Servers sollten regelmäßig aktualisiert werden. Falls die Software nicht den aktuellen Patchstand des Herstellers aufweist, besteht die Gefahr, dass Schwachstellen in dem entsprechenden System vorhanden sind. Besonders kritisch ist der Einsatz von Software, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt wird. Je länger keine Aktualisierung durchgeführt wurde, desto größer ist auch die Wahrscheinlichkeit, dass bereits – teilweise öffentlich verfügbare – Exploits existieren, welche die vorhandenen Sicherheitslücken ausnutzen. Der mögliche Schaden reicht dabei vom Ausfall einzelner Systeme über den Verlust von vertraulichen Daten bis hin zur Korrumpierung des gesamten Netzwerkes. Wir überprüfen daher anhand von ausgelesenen Versionsnummern die Aktualität des entsprechenden Programms.

Verfügbarkeit von administrativen Zugängen

Sofern administrative Zugänge bzw. Fernwartungszugänge zur Verfügung stehen, können Angreifer diese Zugänge nutzen, um weiterführende Angriffe – bspw. aufgrund von Schwachstellen in der eingesetzten Software – durchzuführen. Sofern keine weiteren Maßnahmen ergriffen worden sind, um diesen Angriffen effektiv zu entgegnen, könnte sich der Angreifer erfolgreich auf dem System bzw. der Anwendung anmelden und mit Benutzerrechten interagieren. Erfolgt sogar ein Zugang mit administrativen Rechten, ist das gesamte System korrumpiert. Weiterhin ist der Zugang von ehemaligen Mitarbeitern nutzbar, sofern deren Benutzerkonten noch nicht deaktiviert worden sind. Daher wird die Analyse der automatisierten Scans auch auf administrative Zugänge ausgerichtet.

Verwendung von trivialen Kennwörtern

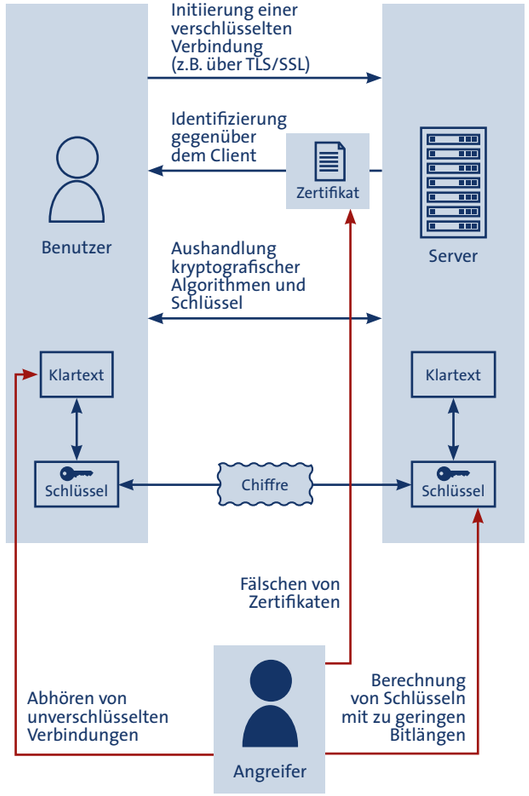
Mit Hilfe von Brute-Force-Methoden wird überprüft, ob triviale Kennwörter verwendet werden. Durch die Nutzung von Trivialkennwörtern besteht auch das Risiko, dass uneingeschränkt auf administrative Bereiche zugegriffen werden kann. Dabei können unter anderem sensible Dateien entwendet sowie kritische Systemeinstellungen manipuliert werden. Weiterhin besteht die Gefahr der kompletten Korrumpierung der Systeme. In diesem Zusammenhang wird auch geprüft, ob ggf. die Standardzugangsdaten des entsprechenden Dienstes einschließlich der Anwendung noch aktiviert sind oder korrekterweise geändert wurden.

Ausgabe von sensiblen Informationen

Im Rahmen der manuellen Tests wird gezielt nach der Ausgabe von sensiblen Informationen gesucht, welche einem Angreifer weiterführende Angriffe erleichtern oder auch erst ermöglichen. Beispielsweise könnte ein Angreifer mit Hilfe der konkreten Versionsnummer eines Dienstes gezielt öffentlich verfügbare Exploits nutzen, um das entsprechende System zu korrumpieren. Beispielsweise ermöglicht die Ausgabe von Konfigurationsdateien, Schwachstellen in der eingesetzten Software ausfindig zu machen.

Test der Verschlüsselung

Sofern Dienste identifiziert wurden, die eine verschlüsselte Kommunikation erlauben, untersuchen wir die Verschlüsselung im Hinblick auf mögliche Fehler. Dabei wird zum einen die Gültigkeit der eingesetzten Zertifikate validiert. Wenn für die Absicherung einer Kommunikation beispielsweise ein selbstsigniertes Zertifikat genutzt wird, ist eine Prüfung der Authentizität des Systems in den meisten Fällen nicht möglich, was die Ausführung von Man-In-The-Middle-Angriffen erleichtert. Zum anderen wird die Angreifbarkeit der eingesetzten Verschlüsselungsverfahren überprüft. Ein potentieller Angreifer mit Zugriff zum Netzwerkverkehr kann die verschlüsselte Kommunikation abhören bzw. aufzeichnen und ggf. durch die Ausnutzung von kryptografischen Schwächen entschlüsseln. Dies ist besonders kritisch, wenn Authentisierungsdaten übermittelt werden. Weiterhin wird untersucht, ob sensible Informationen im Klartext übertragen werden.



Überprüfung von Zugriffsrechten

Durch die fehlende oder unzureichende Überprüfung von Zugriffsberechtigungen kann unter Umständen unberechtigten Personen der Zugriff auf sensible Daten ermöglicht werden. Zudem besteht die Gefahr, dass Systemkonfigurationen manipuliert werden. Daher wird überprüft, ob die identifizierten Dienste und Anwendungen eine adäquate Zugriffsbeschränkung aufweisen.

Test der Netzanmeldung

Sofern wir einen Penetrationstest in Ihrem Intranet durchführen, wird zu Beginn überprüft, ob eine Anmeldung im Unternehmensnetzwerk mit unseren Testsystemen ohne weiteres möglich ist. Falls Sicherheitsmaßnahmen gegen eine unberechtigte Netzanmeldung wie z.B. eine MAC-Filterung umgesetzt sind, wird überprüft, ob diese Maßnahmen umgangen werden können.

Man-In-The-Middle-Angriffe

Im Rahmen von internen Penetrationstests wird geprüft, ob ein Angriff gegen die lokale Netzinfrastruktur möglich ist. Durch einen Man-In-The-Middle-Angriff wird versucht, Verbindungen zu einem Testsystem so umzuleiten, dass die Datenpakete durch unsere Scan-Systeme mitgelesen werden können.

4.2

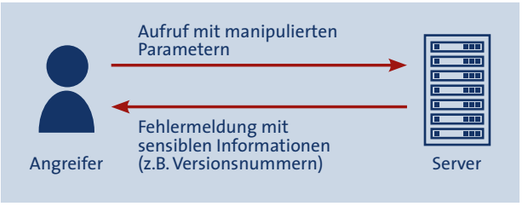
Modul Webapplikationen

Der Aufbau von Webapplikationen wird zunehmend komplexer. Von der E-Mail-Platform bis hin zur Verwaltungssoftware werden wichtige und vor allem sicherheitskritische Programme in das Web respektive in den Browser verlagert. Da die Funktionalität der jeweiligen Anwendung für den Entwickler dabei häufig im Vordergrund steht, sind Sicherheitslücken und Schwachstellen buchstäblich vorprogrammiert.

Unabhängig davon, ob Ihre Anwendung öffentlich oder lediglich im Intranet verfügbar ist, kann ein Penetrationstest mögliche Schwachstellen und Programmierfehler aufdecken, um unberechtigten Zugriffen auf sensible Daten vorzubeugen. Angefangen bei der einfachen Homepage bis hin zum komplexen Online-Shop überprüfen wir in mehrstufigen Tests sowohl die Sicherheit Ihres zugrundeliegenden Webservers als auch der eigentlichen Webapplikation. Dabei werden aufbauend auf automatisierten Port- und Schwachstellenscans anwendungsspezifische manuelle Tests durchgeführt, welche u.a. sämtliche Angriffe der OWASP-Top-10 enthalten.

Auswertung von Fehlermeldungen

Gibt ein System Standardfehlermeldungen aus, werden in der Regel Informationen über die Infrastruktur oder über eingesetzte Programmversionen offen gelegt. Wir suchen daher detailliert nach Fehlermeldungen mit sensiblen Informationen.

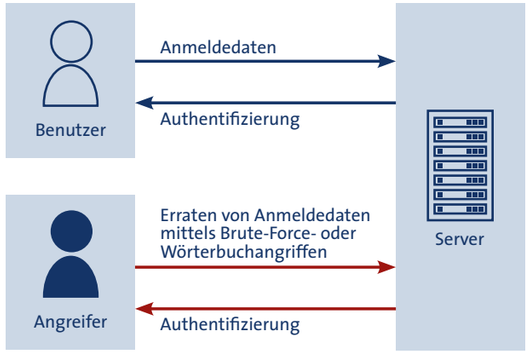


Überprüfung der Verschlüsselung

Vertrauliche Daten wie z.B. Anmelde- oder Bankinformationen sollten grundsätzlich verschlüsselt übertragen werden, um zu verhindern, dass Angreifer den Datenstrom abhören. Es wird daher geprüft, ob alle sensiblen Daten verschlüsselt übertragen und ob ausschließlich aktuelle und sichere Verschlüsselungsverfahren eingesetzt werden.

Überprüfung der Registrierung und Authentisierung

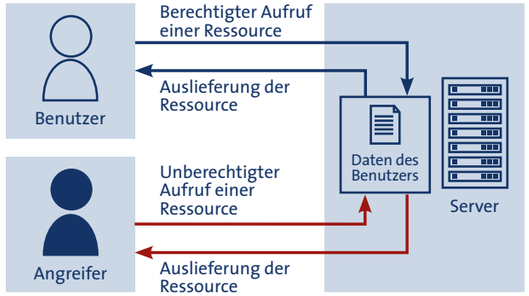
Bei zahlreichen Webseiten besteht die Möglichkeit, sich registrieren zu lassen und mit Hilfe einer Benutzerkennung spezielle Dienste zu nutzen. Im Rahmen des Penetrationstests wird daher die Art und Qualität der Registrierung und Authentisierung geprüft.



Ausweitung der Zugriffsrechte

Über Zugriffsrechte und deren Verwaltung wird sichergestellt, dass der Anwender nur solche Daten lesen und Funktionen ausführen kann, für die er berechtigt ist.

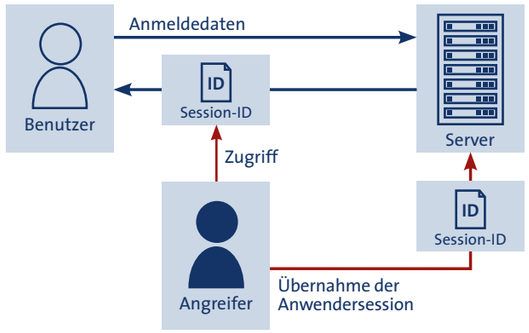
Mit Hilfe von internen und externen Suchfunktionen sowie der Manipulation von Parametern wird versucht, Zugriffsrechte zu umgehen. Im Rahmen einer horizontalen Rechteausweitung wird geprüft, ob auf Daten eines anderen Benutzers zugegriffen werden kann. Ebenso wird auf vertikaler Ebene versucht, Zugriff auf administrative Funktionen und Ressourcen zu erhalten. Über Path-Traversal-Angriffe wird der Zugriff auf Dateien und Verzeichnisse getestet, die nicht zur Veröffentlichung durch den Webserver vorgesehen sind.



Manipulation des Session-Managements

Das http-Protokoll, welches die Kommunikation des Anwenders mit dem Webserver steuert, ist per Definition ein zustandsloses Protokoll, d.h. der Zugriff auf den Webserver ist unabhängig von vorherigen Zugriffen des gleichen Anwenders. Interaktive Webanwendungen müssen daher eine Session-ID verwenden, um den Anwender über mehrere Zugriffe hinweg identifizieren zu können. Um zu vermeiden, dass ein Anwender die Identität eines anderen Nutzers vortäuscht und dessen Sitzung übernimmt, müssen die genutzten Session-IDs ausreichend zufällig sein.

Bei der Überprüfung des Session-Managements wird versucht, durch Veränderung der Verbindungsdaten (URL, Verbindungsparameter, Session-ID) die Daten einer bestehenden Session zu verwenden und diese zu übernehmen.

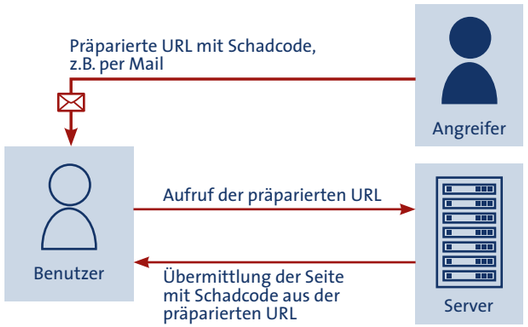


Cross-Site-Scripting (XSS)

Beim Cross-Site-Scripting manipuliert der Angreifer eine Webseite und fügt neue Inhalte hinzu, die dann von einem anderen Benutzer gelesen werden. Wenn es sich bei dem eingefügten Inhalt um einen Programmcode, z.B. JavaScript, handelt, wird dieses Programm auf dem System des Benutzers ausgeführt.

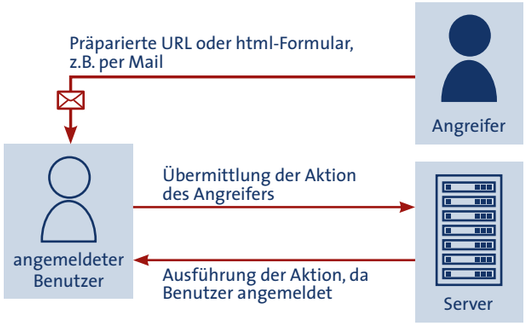
Sofern die mit Schadcode versehene Webseite über einen Browser aufgerufen wird, der mit besonderen Sicherheitsrechten bzw. Privilegien ausgestattet ist, kann der installierte Schadcode in Abhängigkeit von dem Funktionsumfang der Skriptsprache mit den Rechten des lokalen Benutzers ausgeführt werden, möglicherweise sogar mit Administrator-Rechten. Selbst wenn der Browser ohne weitere Privilegien betrieben wird, können Cross-Site-Scripting-Angriffe dazu genutzt werden, die Session-ID eines Benutzers auszulesen.

Beim Cross-Site-Scripting wird zwischen Angriffen unterschieden, die vom Benutzer selbst durch den Aufruf von präparierten Links initiiert werden (reflected XSS) und Angriffen, die persistent im Webauftritt gespeichert sind und von jedem Besucher einer Webseite ausgeführt werden (stored XSS). Im Rahmen des Penetrationstests werden beide Angriffstechniken getestet.



Cross-Site-Request-Forgery (CSRF)

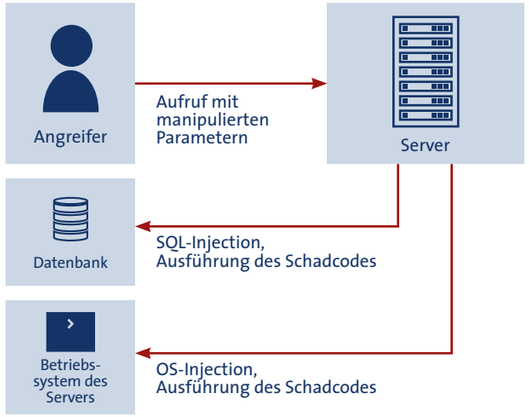
Bei einer seitenübergreifenden Aufruf-Manipulation (Cross-Site-Request-Forgery) wird eine Aktion im Browser eines bereits angemeldeten Benutzers mit dessen Rechten ausgeführt. Ähnlich dem Cross-Site-Scripting wählt der Angreifer die Anfrage so, dass bei ihrem Aufruf die Webanwendung die vom Angreifer gewünschte Aktion ausführt. Dies könnte beispielsweise das Hinzufügen eines neuen Benutzers oder das Ändern des Kennwortes sein.



Injection

Injection ist ein Sammelbegriff für das Ausnutzen einer Sicherheitslücke, bei der Schadcode an eine Webapplikation übermittelt wird, welcher anschließend durch fehlerhafte Weiterverarbeitung oder unzureichende Überprüfung von Metazeichen durch den Webserver ausgeführt wird. Ziel ist es, Daten auszulesen, zu verändern oder Kontrolle über den Server zu erhalten. Während bei einer SQL-Injection versucht wird, Datenbankbefehle einzuschleusen, wird bei einer OS-Injection die Webapplikation dazu genutzt, Betriebssystembefehle mit den Rechten des Webservers auszuführen.

Bei einer Header-Injection wird der Responseheader manipuliert, um beispielsweise den Benutzer auf eine Phishingseite umzuleiten. Die Anfälligkeit für Injections wird durch eine automatische und manuelle Eingabe von entsprechenden Zeichenketten im Anmeldefenster oder in Suchmasken überprüft.



4.3

Modul Industrieanlagen

Die sogenannte Smart Factory – die Fabrik der Zukunft – soll Produktionsprozesse intelligenter und vor allem effizienter gestalten, indem alle Geräte, Bauteile und Mitarbeiter miteinander vernetzt sind. Im Rahmen der 4. Industriellen Revolution werden einfach vernetzte technische Systeme – aufbauend auf dem Internet der Dinge – zu sogenannten Cyber-Physical Systems erweitert. Diese weltweite Verbindung von Maschinen, Lagersystemen und Betriebsmitteln existiert bereits in allen kritischen Infrastrukturen, wie z.B. im Energie-, Wasser-, Transport- und Gesundheitssektor.

Für die Sicherheit dieser Anlagen sind grundlegend zwei Aspekte von großer Bedeutung: Zum einen muss die Betriebssicherheit betrachtet werden, damit die Systeme keine Gefahr für Menschen und Umgebung darstellen. Auf der anderen Seite muss jede ans Internet angeschlossene Maschine vor unbefugten Zugriffen und Manipulationen geschützt werden. Im Zuge der Vernetzung werden in diesem Zusammenhang auch neue Angriffsvektoren für potentielle Hacker und Datendiebe geschaffen. Dass die Cyber-Sabotage in der Automatisierungsindustrie dabei ein ernst zu nehmendes Thema ist, zeigen nicht zuletzt die öffentlich bekannt gewordenen und äußerst gefährlichen Schad-Programme, wie z.B. Stuxnet, Duqu oder Flame.

Um die Sicherheit Ihrer IT-Systeme zu gewährleisten und möglichen Cyber-Angriffen und Datendiebstählen vorzubeugen, ohne auf die Vorteile der Vernetzung zu verzichten, können wir Sie durch speziell angepasste Penetrationstests sowie durch die Erstellung von Sicherheitskonzepten unterstützen. Dabei halten wir uns an international anerkannte Standards und prüfen u.a. die BSI Top 10 für ICS, d.h. die vom BSI veröffentlichten zehn größten Bedrohungen für Industrial Control Systeme.

Überprüfung der ICS-Komponenten

Jede Komponente im ICS-Netz, angefangen vom einfachen Anwendungsserver bis hin zum komplexen Industrieautomaten, kann Schwachstellen und Sicherheitslücken enthalten. Zudem werden viele Systeme oft in einer unzureichend gesicherten Konfiguration betrieben. Wir prüfen, ob alle kritischen IT-Komponenten ausreichend abgesichert sind, um erfolgreiche Angriffe zu verhindern. Dies beinhaltet auch eine Überprüfung der Software-Aktualität und des Patch-Managements. Weiterhin testen wir, ob auch normale Netzwerkkomponenten wie z.B. Router und Switches durch Angreifer manipuliert werden können, um beispielsweise Man-In-The-Middle- oder Sniffing-Attacken durchzuführen.

Test der Kommunikation

Nicht nur im Internet der Dinge, sondern auch bei traditionellen technischen Systemen erfolgt die Kommunikation heute mehr und mehr auf der Basis von TCP-basierten Internettechniken. Da zudem typische Protokolle wie IEC 60870-5-104 kaum Sicherheitsfunktionen bieten und eine kryptografische Absicherung meist unsicher implementiert ist, können unter anderem sensible Authentisierungsdaten, Schaltbefehle und Zustandsinformationen durch potentielle Angreifer ausgelesen werden. Daher testen wir Ihre implementierten Maßnahmen zur Sicherstellung der Vertraulichkeit und der Authentizität auf dem Übertragungskanal. Diese Prüfungen umfassen sowohl TCP/IP-basierte Verbindungen sowie ggf. serielle Funksignale zwischen Kontrollzentren und Außenstationen.

Prüfung von Zugriffsberechtigungen

Durch die Überprüfung von vertikalen sowie horizontalen Zugriffsberechtigungen testen wir die Möglichkeiten für unberechtigte Zugriffe auf Ressourcen durch potentielle Innentäter. Weiterhin prüfen wir die Zugriffsmöglichkeit von außen durch externe Tests. Dabei stehen vor allem Methoden zur Authentisierung und Autorisierung im Vordergrund. Zusätzlich erfolgt die Kontrolle der physischen Zutrittsberechtigungen, um das Einschleusen von Schadcode sowie die Infektion mit Malware über externe Wechseldatenträger und Hardware auszuschließen.

Test der Systemredundanz

Durch sogenannte (distributed) Denial-of-Service-Angriffe, d.h. (verteilte) Dienstblockaden, können die Verbindungen innerhalb Ihres ICS-Netzwerkes sowie der Zugriff auf benötigte Ressourcen erheblich beeinträchtigt werden. Dies kann im ungünstigsten Fall zum totalen Ausfall der Produktionsanlage führen. Daher überprüfen wir, ob die Möglichkeit besteht, dass bestimmte Systeme zum Absturz gebracht werden können und ob genügend Redundanzen bestehen, um einen Single-Point-of-Failure zu vermeiden.

4.4

Modul Produkt-Hacking

Die Zeiten, in denen PCs die Nutzung des Internets dominierten, sind vorbei. Eine Vielzahl von vernetzten Produkten ist bereits heute Teil unseres Alltags. Medien berichten regelmäßig über neue, teils exotische Beiträge zum „Internet of Things“, dem Internet der Dinge. Die längst üblichen Smartphones werden neuerdings ergänzt durch Wearables wie Smart Watches und Fitnesstracker. Das Smart Home ermöglicht eine bedarfsgerechte Steuerung von Heizung und Beleuchtung sowie eine Verbrauchsdatenerfassung von Strom, Wasser und Gas über Smart Meter. Autos sind mit GPS, GSM, WLAN und Bluetooth vernetzter denn je.

All diese Produkte und die auf ihnen verarbeiteten oder gespeicherten Daten sind durch Schnittstellen ins Heimnetzwerk, Mobilfunknetz oder ins Internet ständig dem Risiko des externen missbräuchlichen Zugriffs ausgesetzt. Berichte über Car Hacking oder Schwachstellen in Smartphones haben gezeigt, dass das Thema Produkt-Hacking eine große Bedeutung für die Öffentlichkeit hat.

Für die Validierung der Sicherheit von Produkten, vom kleinsten Gadget über die Waschmaschine bis hin zum Auto sind wir Ihr kompetenter Ansprechpartner. Wir führen für Sie individuell angepasste Penetrationstests durch oder erstellen Sicherheitskonzepte.

Prüfung der Schnittstellensicherheit

Schnittstellen bilden die Basis der Kommunikation mit dem Produkt. Gerade drahtlose Schnittstellen bieten eine beliebte Angriffsfläche, da Angriffe von außen keinen physischen Zugriff auf das Gerät voraussetzen. Häufige Schnittstellen

sind z.B. Bluetooth, NFC (RFID), Mobilfunknetz (GSM) oder Webschnittstellen per WLAN. Wir überprüfen die Sicherheit der Schnittstellen und ihre Konfiguration hinsichtlich missbräuchlichem Zugriff sowie auf mögliche Schwachstellen in den verwendeten Protokollen und Diensten.

Absicherung der Kommunikation

Gerade drahtlose Kommunikation lässt sich leicht abhören. Deshalb ist eine verschlüsselte Kommunikation zwischen Geräten und dem Heimnetz oder dem Internet erforderlich. Wir überprüfen die verwendeten Verschlüsselungsalgorithmen und ihre Parameter auf ihre Wirksamkeit und Sicherheit gegen kryptographische Angriffe.

Test der Zugriffskontrolle

Wie authentifiziert sich der Benutzer gegenüber dem Produkt? Gibt es verschiedene Benutzerrollen (Administrator, Benutzer, Gast) und wird ihre Trennung eingehalten? Durch eine Überprüfung der vertikalen sowie horizontalen Zugriffsberechtigungen testen wir zum einen, ob sensible Daten unberechtigt manipuliert werden können. Zum anderen wird geprüft, ob Konfigurations- und Firmware-Einstellungen auf dem entsprechenden Gerät geändert werden können.

4.5

Sondermodule

Neben unseren Standard-Testmodulen können Sie mit uns selbstverständlich individuelle und speziell auf Ihre Bedürfnisse zugeschnittene Testszenarien abstimmen. Dabei wären beispielsweise die folgenden Testziele denkbar:

- Überprüfung der WLAN-Sicherheit, was sowohl die eingesetzten Authentisierungs- und Verschlüsselungsmethoden als auch die Konfiguration der Access Points umfasst
- Penetrationstests von SOAP- oder REST-basierten Webservices sowie API-Schnittstellen
- Sicherheitsanalyse eines mobilen Clients, um die Zugriffsmöglichkeiten auf sensible Daten bei Verlust oder Diebstahl des Systems zu bestimmen
- Erstellung eines Sicherheitskonzeptes für die Nutzung von iOS- oder Android-Smartphones
- Konzeptionelle Überprüfungen, angefangen bei der Gebäude- und Netzwerksicherheit bis hin zur Überprüfung von Dienstleisterverträgen

05.

Kalkulation und Produktvorschläge

Nachdem wir in den vorherigen Kapiteln unsere Vorgehensweise, die Testszenarien sowie die Testmodule und Prüfthemen ausführlich dargestellt haben, möchten wir Ihnen im Folgenden eine möglichst konkrete Aufwandsabschätzung für einzelne Testmodule geben. Der Prüf- und Dokumentationsaufwand für das Netzwerk-Modul hängt beispielsweise von der Anzahl der zu testenden Systeme ab. Beim Webapplikationsmodul bestimmt die Komplexität der Anwendung den Aufwand des Penetrationstests.

5.1

Modul Netzwerke

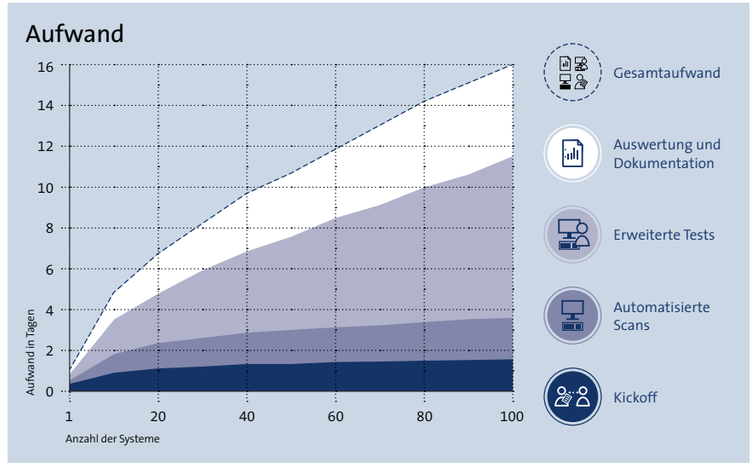
Sofern ein größerer IP-Adressbereich als Testziel gewählt wird, erhöht sich zwar die Dauer der automatisierten Scans, der eigentliche Arbeitsaufwand hängt allerdings von der Anzahl der Systeme ab.

Der Aufwand für die Ergebnispräsentation liegt in der Regel bei einem zusätzlichen Arbeitstag. Die Überprüfung der getroffenen Gegenmaßnahmen hängt vom Umfang der Maßnahmen ab und kann daher erst nach Abschluss des entsprechenden Arbeitspaketes kalkuliert werden.

Bei der Wiederholung eines Penetrationstests können je nach Testfrequenz und Prüfgegenstand in der Regel bis zu 50 Prozent des Gesamtaufwands entfallen.

Um weiteren Aufwand zu sparen, können Sie neben der Testfrequenz zudem die Prüftiefe frei wählen und Ihren individuellen Penetrationstest zusammenstellen. Die folgende Tabelle zeigt mögliche Produkte:

Produktvorschläge	Security Scan	Externer Penetrationstest	Externer Penetrationstest Plus	Interner Penetrationstest	Interner Penetrationstest Plus
Portscan	✓	✓	✓	✓	✓
Schwachstellenscans	✓	✓			
Auswertung und Validierung der Scan-Ergebnisse		✓	✓	✓	✓
Manuelle Prüfungen 1. Einsatz veralteter Software 2. Verfügbarkeit von administrativen Zugängen 3. Verwendung von trivialen Kennwörtern 4. Ausgabe von sensiblen Informationen 5. Test der Verschlüsselung 6. Überprüfung von Zugriffsrechten		✓	✓	✓	✓
Test der Netzanmeldung				✓	✓
Man-In-The-Middle-Angriffe				✓	✓
Post-Exploitation (aktive Ausführung von Angriffen)			✓		✓
Social-Engineering/Phishing-Kampagnen			✓		✓
Detaillierte Dokumentation mit Empfehlungen		✓	✓	✓	✓
Präsentation der Ergebnisse			✓		✓



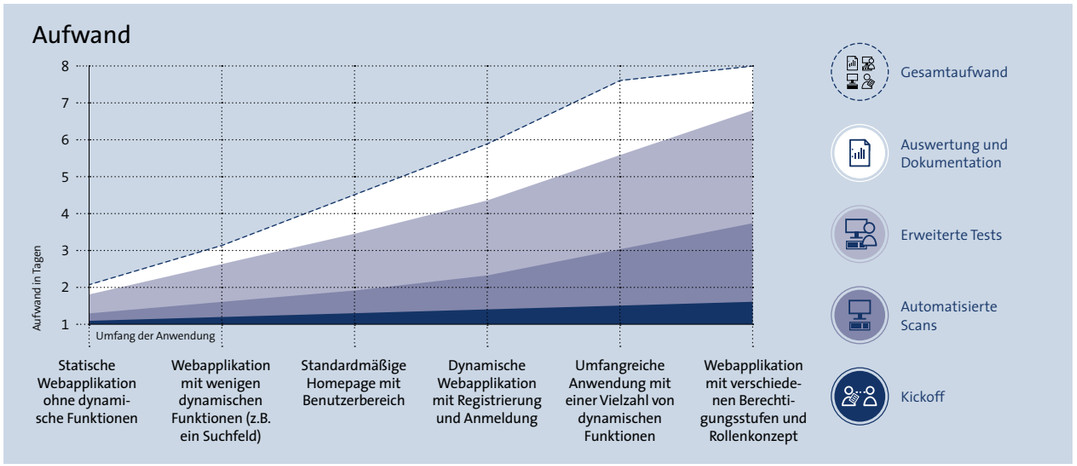
5.2

Modul Webapplikationen

Analog zum Netzwerk-Modul liegt der Aufwand für die Ergebnispräsentation üblicherweise bei einem Arbeitstag. Die Überprüfung der getroffenen Gegenmaßnahmen hängt ebenfalls vom Umfang der Maßnahmen ab und kann daher erst nach Abschluss des entsprechenden Arbeitspaketes kalkuliert werden.

Je nach Testfrequenz und Prüftiefe können zudem die Aufwände individuell mit Ihnen abgestimmt werden. Im Folgenden finden sich verschiedene Produktvorschläge:

Produktvorschläge	Security Scan	Penetrationstest	Penetrationstest Plus
Portscan	✓	✓	✓
Schwachstellenscans	✓	✓	✓
Scan der Webapplikation	✓	✓	✓
Auswertung und Validierung der Scan-Ergebnisse		✓	✓
Manuelle Prüfungen 1. Auswertung von Fehlermeldungen 2. Überprüfung der Verschlüsselung 3. Überprüfung der Registrierung und Authentisierung 4. Ausweitung der Zugriffsrechte 5. Manipulation des Session-Managements 6. Cross-Site-Scripting (XSS) 7. Cross-Site-Request-Forgery (CSRF) 8. Injection		✓	✓
Post-Exploitation (aktive Ausführung von Angriffen)			✓
Detaillierte Dokumentation mit Empfehlungen		✓	✓
Präsentation der Ergebnisse			✓



datenschutz nord Gruppe

Die datenschutz nord Gruppe, die sich aus der **datenschutz nord GmbH**, der **datenschutz süd GmbH**, der **datenschutz cert GmbH** und der **FIRST PRIVACY GmbH** zusammensetzt, hat sich auf Dienstleistungen im Bereich des Datenschutzes und der Informationssicherheit spezialisiert.

Eines unserer Hauptbetätigungsfelder ist der betriebliche Datenschutz, den wir für über 300 Firmen wahrnehmen; sowohl für Großkonzerne als auch für mittelständische Unternehmen und Unternehmen der öffentlichen Verwaltung, u.a. Einzelhandelskonzerne, Pharmaunternehmen, Energieversorger, Werbeagenturen, aber auch Krankenhäuser und Universitäten.

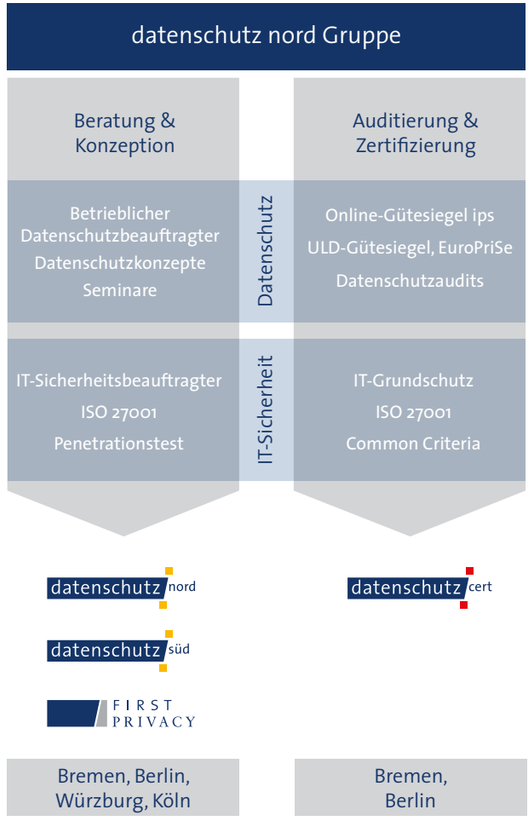
Als IT-Sicherheitsbeauftragter sind wir ebenso in vielen Unternehmen tätig. Unsere Sicherheitsexperten führen umfangreiche Penetrationstest durch und beraten Sie bei ISO 27001.

Wir sind beim Unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein, beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und bei der Bundesnetzagentur anerkannt sowie bei der Deutschen Akkreditierungsstelle (DAkkS) als Zertifizierungsstelle akkreditiert. Damit zählt die datenschutz nord Gruppe bundesweit zu den führenden Anbietern im Bereich Datenschutz und Informationssicherheit.

Wir hoffen, Ihnen mit der vorliegenden Broschüre einen umfassenden Überblick über Penetrationstests gegeben zu haben. Kontaktieren Sie uns!

Ihr Team der datenschutz nord Gruppe

Unsere Geschäftsfelder










01/dsn

datenschutz nord GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88
28217 Bremen

Niederlassung Berlin-Mitte
Reinhardtstraße 46
10117 Berlin

Tel.: 0421 69 66 32 0
office@datenschutz-nord.de
www.datenschutz-nord.de

datenschutz süd GmbH

Hauptsitz Würzburg
Wörthstraße 15
97082 Würzburg

Niederlassung Köln
Eupener Str. 165
50933 Köln

Tel.: 0931 30 49 76 0
office@datenschutz-sued.de
www.datenschutz-sued.de

datenschutz nord

datenschutz süd