secunet

Whitepaper

Penetrationstests und Sicherheitsanalysen

Inhaltsverzeichnis

Version 1.0 - Stand Juli 2013

1 Überblick

Das vorliegende Dokument beschreibt das grundlegende Vorgehensmodell der secunet Security Networks AG bei der Durchführung von technischen Sicherheitsanalysen (auch Penetrationstests oder kurz Pentests genannt).

Es informiert über den Rahmen und die Art und Weise, wie eine technische Sicherheitsanalyse bei einem Auftraggeber durchgeführt werden kann. Dabei liegt der Schwerpunkt auf der Beschreibung eines möglichen Vorgehens.

In einem weiteren, bei der secunet erhältlichen Dokument, ist in einem Beispielreport aufgeführt, wie die im Rahmen einer technischen Sicherheitsanalyse gesammelten Ergebnisse ausgewertet und dokumentiert werden. Eine kurze Beschreibung der Inhalte eines solchen Reports befindet sich im sechsten Kapitel dieses Dokuments.

2 Einleitung

IT-Systeme und -Netzwerke sind das „Gehirn“ eines Unternehmens: Hier werden alle wichtigen Informationen und Daten zu Kunden, Mitarbeitern, Produkten und Aufträgen erfasst, bearbeitet und gespeichert. Mittlerweile sind Geschäftsprozesse weitestgehend durch Informationstechnik unterstützt und getrieben, so dass Sicherheitsprobleme an dieser Stelle bereits kritisch sind und mit zunehmender Technisierung immer kritischer werden: Werden die Geschäftswerte eines Unternehmens in Bezug auf ihre Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) verletzt, ist der Geschäftszweck bis zur Lösung des Problems oft nicht mehr zu erbringen. Umso wichtiger ist es, die zugrundeliegende Infrastruktur zu schützen. Oft wissen Unternehmen allerdings gar nicht, dass ihr Netzwerk Schwachstellen aufweist oder wo danach zu suchen wäre. Mit einer technischen Sicherheitsanalyse können diese möglichen Angriffspunkte aufgedeckt werden.

Dazu wird mit dem Auftraggeber zunächst die generelle Vorgehensweise abgestimmt: Beim Whitebox-Test erhält das Analyseteam Details über das Netzwerk, beim Blackbox-Test hingegen geht es wie ein tatsächlicher Angreifer vor, der kaum Informationen über das System hat (vgl. Kapitel 3.1). In diesem Fall verwenden die Experten der secunet selbst entwickelte und frei erhältliche Tools, um sich trotz der dürftigen Informationen Zugang zum Netzwerk zu verschaffen.

Einmal im Netzwerk, verschaffen sie sich zunächst einen Überblick über die Strukturen (vgl. Kapitel 3.3). Anschließend greifen sie die einzelnen Netzwerkkomponenten an. Dazu ermitteln die Experten anhand verschiedener Merkmale ein Ranking der Ziele, deren Schwachstellen am einfachsten auszunutzen sind (vgl. Kapitel 3.5 und 3.6). Selbstverständlich kann der Auftraggeber auch die Komponenten nennen, die einer Detailanalyse unterzogen werden sollen. Auch hier kommen wieder speziell entwickelte und angepasste Tools zum Einsatz.

Auf Wunsch können nach den technischen Analysen des Netzwerks weitere Analysen durchgeführt werden. Denn nicht nur schwache Systeme im Netzwerk selbst können das Ziel von Angriffen sein: Auch offene WLAN-Verbindungen, der Netzverkehr selbst und die eigenen Mitarbeiter können als Schwachstellen ausgenutzt werden (vgl. Kapitel 4).

Wichtig bei allen Analysen eines Netzwerks ist die Aufrechterhaltung des ungestörten alltäglichen Geschäftsbetriebs. Auf Wunsch werden die Analysen auch außerhalb der üblichen Arbeitszeiten durchgeführt, um die Sicherheitsanalyse komplett vom aktiven Geschäftsbetrieb zu entkoppeln.

3 Das Vorgehensmodell

„Jeder IT-Verbund ist einzigartig.“

„Die Anforderungen der Kunden an eine technische Sicherheitsuntersuchung sind von Fall zu Fall unterschiedlich.“

Auf diese zwei kurzen Sätze lässt sich die Erfahrung der letzten fünfzehn Jahre bei der Durchführung von technischen Sicherheitsanalysen zusammenfassen. Tatsache ist, dass es keine Analyse gibt, die exakt einer anderen gleicht. Dafür bestimmen zu viele Faktoren die Untersuchungen, die von den Projektteilnehmern (sowohl auf Kunden- als auch auf Auftragnehmerseite) nicht beeinflusst werden können:

- Netzwerkstrukturen, Segmentierung, Anbindung an andere Netze
- aktive Netzwerkkomponenten (Router, Switches, Firewalls)
- genutzte Betriebssysteme
- genutzte Anwendungsprogramme
- proprietäre Software
- Patch-Stände (Hardware & Software)
- kritische Anwendungen, die von der Analyse ausgegrenzt werden müssen
- uvm.

Allein aus dieser Auflistung wird klar, dass jede Analyse individuell an die jeweiligen Rahmenbedingungen angepasst werden muss. Bestimmte Vorgehensmuster müssen verworfen, eigene Tools erstellt und die Ergebnisse neu korreliert und ausgewertet werden.

Das vorliegende Konzept kann daher nur das generelle Vorgehen bei einer technischen Sicherheitsanalyse beschreiben. Um trotzdem einen Eindruck der Tätigkeiten zu bekommen, kann zusätzlich zu diesem Dokument ein Beispielbericht angefordert werden. In diesem wird ein fiktives Unternehmen untersucht und die Ergebnisse dokumentiert.

In Abbildung 1 ist das Schema des Vorgehensmodells skizziert. Die einzelnen Begriffe und Handlungsmöglichkeiten werden in diesem und den folgenden Kapiteln beschrieben.

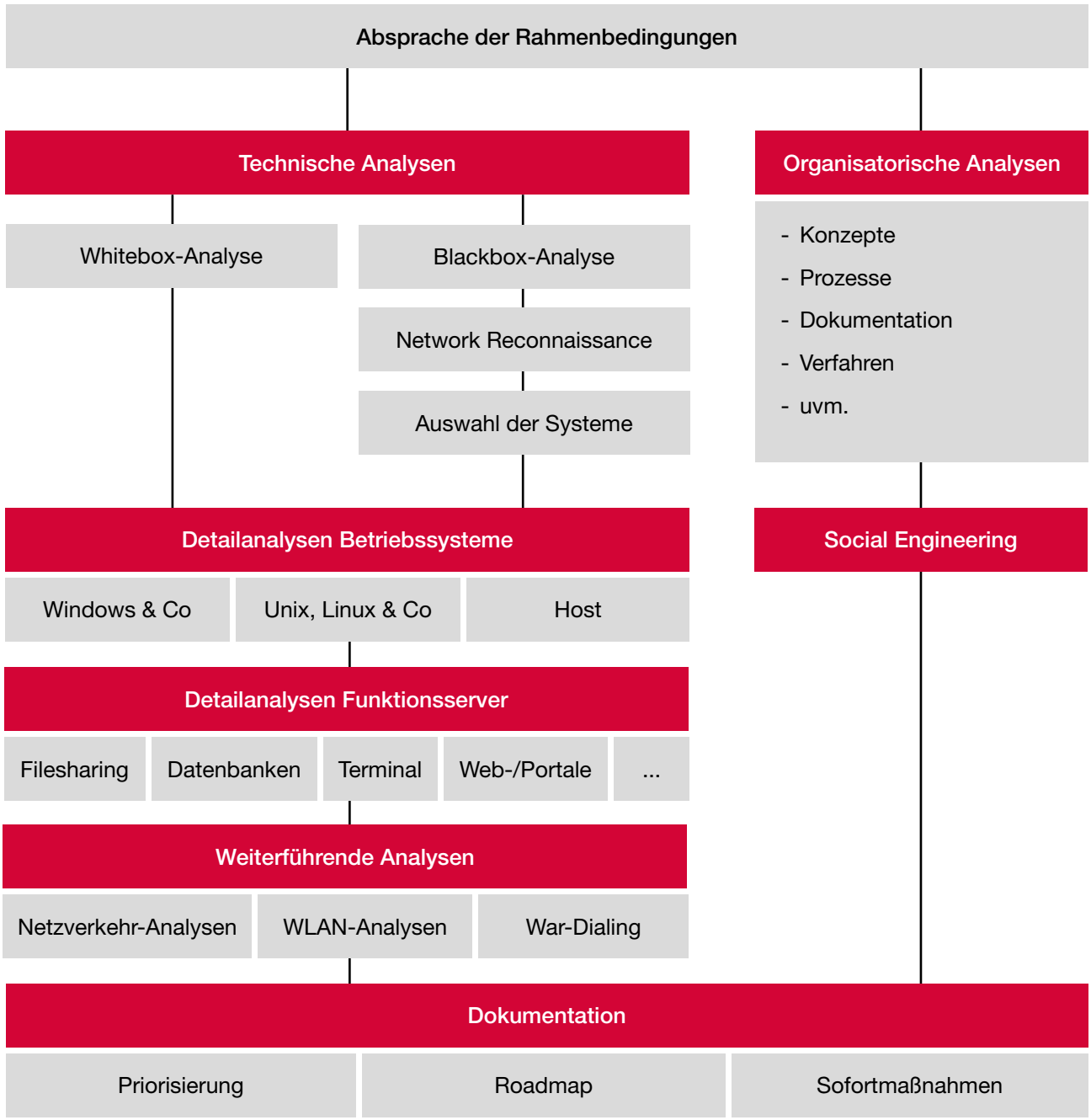


Abbildung 1: Schematische Darstellung des Vorgehens

3.1 Blackbox- vs. Whitebox-Tests

Im Zusammenhang mit technischen Sicherheitsanalysen tauchen immer wieder die Begriffe Whitebox- und Blackbox-Tests auf. Diese Begriffe werden zudem in unterschiedlicher Art und Weise verwendet, so dass an dieser Stelle eine kurze Erklärung notwendig ist. Im Rahmen dieses Konzepts wird unter einem **Blackbox-Test** ein Test **ohne weitere Detailkenntnis über das Untersuchungsziel** verstanden. Bei einem Blackbox-Test wird im Allgemeinen nur ein Name, eine Internet-Domäne oder eine IP-Adresse bereitgestellt. Teilweise wird eine Visitenkarte als einziges Hilfsmittel zugestanden. Alle weiteren Informationen über das Zielobjekt müssen beschafft werden, wie es ein Angreifer machen würde, der eben diese Visitenkarte gefunden hat. Es wird hier ein externer Täter simuliert, der keine Informationen über das Zielobjekt hat.

Bei einem **Whitebox-Test** hingegen stehen dem Analyseteam **Informationen über das Zielobjekt** zur Verfügung. Je nach Absprache sind dies Netzwerkpläne, Betriebskonzepte und sogar administrative Authentisierungsmerkmale. Bei einem Whitebox-Test wird daher eher ein Innentäter simuliert, der nahezu beliebigen Zugriff auf interne Ressourcen hat.

3.2 Randbedingungen

Technische Sicherheitsanalysen werden von der secunet in enger Abstimmung mit dem Auftraggeber durchgeführt. Weder durch den Auftraggeber noch durch den Auftragnehmer können sämtliche Implikationen, die eine Analyse nach sich ziehen kann, im Vorfeld komplett überblickt werden. Dazu sind Systemlandschaften zu unterschiedlich und die Wechselwirkungen zwischen Systemen zu umfangreich. Auch können sich während der laufenden Analyse neue Informationen und somit Ziele und Analyseschritte ergeben, die nicht abzusehen waren.

Umso wichtiger ist es, dass zwischen dem Auftragnehmer und dem Auftraggeber schnelle und zuverlässige Kommunikationswege etabliert sind. Vor der Durchführung einzelner Angriffe wird immer Rücksprache mit dem Auftraggeber gehalten. So wird verhindert, dass kritische oder außerhalb der geplanten Reichweite liegende Ziele in die Analyse einbezogen werden. Die secunet legt zudem ein besonderes Augenmerk auf die Einhaltung existierender gesetzlicher Regelungen (Hackerparagraph), damit die Tätigkeiten im Rahmen der technischen Sicherheitsanalyse für keine der Parteien juristische Folgen haben.

3.3 Network Reconnaissance

Der Begriff Network Reconnaissance beschreibt die Art, wie der Überblick über ein Netzwerk gewonnen wird. Meist haben die durchführenden Mitarbeiter bei einer technischen Sicherheitsanalyse keinen Netzplan des zu untersuchenden Zielobjekts. Das Ziel der Network Reconnaissance ist es also, das Untersuchungsobjekt etwas detaillierter zu erkunden:

3.3.1 Vorgehen: Interne Analysen

Je nach vorliegenden Informationen muss sich das durchführende Untersuchungsteam zunächst einen Zugang zum Untersuchungsobjekt verschaffen. Hierzu gehört häufig auch die Bestimmung einer geeigneten Netzkennung (IP-Adressen, Subnetzmasken, etc.).

Mittels passiver Analyse werden innerhalb des Netzes, für das ein Anschluss gelegt wurde, übertragene IP-Pakete abgehört und analysiert. Im Falle von WLAN-Untersuchungen kann sich diese Analyse auch auf das Entschlüsseln von übertragenen IP-Paketen beziehen.

Ausgehend von den übertragenen Netzwerkpaketen wird eine eigene Adresse gewählt. Für den Fall, dass Einbruchserkennungssysteme (IDS = Intrusion Detection Systems) vermutet werden, kann dann z. B. die eigene Netzkennung so weit verschleiert werden, dass eine Entdeckung des angreifenden Systems eingeschränkt wird (beispielsweise durch die Änderung der eingesetzten MAC-Adressen).

3.3.1.1 Tools und Techniken

Je nach Untersuchungsgegenstand kann bereits die Protokollierung des Netzwerkstroms dazu führen, dass sämtliche Strukturen erkundet werden. Zum Beispiel konnten während einer Untersuchung Kommunikationspakete unterschiedlicher Router abgehört werden, die unverschlüsselt die lokal genutzten Netzsegmente übertragen haben. In anderen Fällen, in denen zunächst nur ein Segment identifiziert werden konnte, mussten diese Informationen mit aufwendigen IP-Scans (beispielsweise mittels Portbunny) erschlossen werden.

Neben der Analyse der verwendeten Netzbereiche werden während der Network Reconnaissance auch die erreichbaren Systeme, die auf den Systemen genutzten Dienste und die verwendeten Betriebssysteme identifiziert. Diese Informationen werden benötigt, um die erkannten Netze grob zu klassifizieren. Es hat sich gezeigt, dass viele untersuchte Objekte nicht sonderlich stark oder auch gar nicht segmentiert und Server und Clientnetze funktional oft durch beispielsweise Firewalls getrennt sind. Dennoch sind häufig Strukturen (zum Beispiel die Reservierung der ersten 50 Adressen in einem Class-C Netz für Server und aktive Netzkomponenten) anhand der gesammelten Daten erkennbar.

Mit der internen Analyse wird das Ziel der Network Reconnaissance erreicht, einen Strukturplan der intern genutzten Netze und nach Möglichkeit der verwendeten Systeme zu erlangen. Mittels dieses Plans kann dann das weitere Vorgehen sowohl im Analyseteam als auch mit dem Auftraggeber bestimmt werden.

3.3.2 Vorgehen: Externe Analysen

Bei Analysen über das Internet lassen sich Informationen nicht auf passivem Weg sammeln. Entsprechend muss in diesem Fall ein offensiveres Vorgehen gewählt werden:

Zunächst werden mittels eines Portscans die erreichbaren Systeme identifiziert. Der Portscan geht über alle IP-Adressen im Zielbereich – unabhängig davon, ob das System via ICMP Echo-Request (PING) erreichbar ist oder nicht.

Die Ergebnisse des Portscans werden in ein automatisches Überwachungssystem eingepflegt, das während des kompletten Tests die Erreichbarkeit der identifizierten Ports überprüft – so können Ausfälle einzelner Komponenten schnell erkannt werden.

3.3.2.1 Tools und Techniken

Nachdem die Überwachung der Systemerreichbarkeit sichergestellt und die Ports identifiziert sind, über die das Zielsystem kommunizieren kann, werden die auf diesen Ports genutzten Programme identifiziert und Schwachstellen in diesen Programmen gesucht.

Dazu wird ein Schwachstellenscan mit dem Tool Nessus durchgeführt. Das Tool wird in der jeweils neuesten Version mit den tagesaktuellen Plugins verwendet.

Im Anschluss werden die identifizierten Schwachstellen manuell genauer untersucht. In Rücksprache mit dem Auftraggeber werden die für einen Angriff Erfolg versprechendsten ausgenutzt, um weitere Informationen über das Zielsystem zu erhalten.

Je nach Analyseumfeld werden neben Nessus auch noch weitere Schwachstellenscanner eingesetzt (beispielsweise NexPose oder OpenVAS). Das Vorgehen ist bei allen Scannern jedoch das gleiche:

- Alle Ports auf allen Systemen werden überprüft.
- Schwachstellen werden aufgelistet, Schwachstellen jedoch ausschließlich nach Rücksprache mit dem Auftraggeber ausgenutzt.
- Denial-of-Service-Tests sind ausgeschlossen.
- Mit Ausnahme von Log-Daten werden lokal keine Daten geändert.

3.4 Auswahl geeigneter Systeme

Ist das zur Verfügung stehende Budget eines technischen Audits nicht groß genug für eine detaillierte Untersuchung aller innerhalb des untersuchten Objekts erreichbaren Systeme, muss das Analyseteam (ggf. in Abstimmung mit dem Auftraggeber) bestimmen, welche Ziele für eine detaillierte manuelle Analyse (vgl. Kapitel 3.5) lohnenswert sind. Ein ähnliches Verhalten würde auch ein bösartiger Angreifer verfolgen:

- Identifikation des schwächsten Systems
- Zugriff auf dieses System
- Nutzung der Informationen auf diesem System zur Angriffsvorbereitung auf weitere Systeme

Um eine Auswahl der lohnendsten Ziele zu ermöglichen, wird ein Ranking der erreichbaren Systeme erstellt. In dieses Ranking fließen verschiedene Bewertungskategorien mit unterschiedlicher Gewichtung ein (zum Beispiel wird der Punkt ‚verfügbare Authentisierungsinformationen' deutlich stärker gewichtet als der Punkt ‚Anzahl ähnlicher Systeme'):

- Vorgaben des Auftraggebers (Zielsysteme, zu sammelnde Daten, etc.)
- Betriebssystem
- Anzahl ähnlicher Systeme
- Ergebnisse des Portscans und eines automatisierten Schwachstellenscans
- Potenziell zu erwartende Daten (Fileserver, Datenbank, Workstation)
- Verfügbare Authentisierungsinformationen

Ziel dieses Arbeitsabschnittes muss sein, die benötigten Informationen zu erlangen.

3.4.1 Vorgehen

Zur effizienten Sammlung der notwendigen Informationen wird in diesem Arbeitsabschnitt ein Mix aus größtenteils automatisierten Schwachstellenscannern eingesetzt, die anhand von aktuellen Datenbanken und Paketsignaturen erkennen, welche Softwarepakete auf einem System installiert sind, wie der Patchstand der eingesetzten Software ist etc.

Anhand der im Bereich Network Reconnaissance gesammelten Informationen werden die genutzten Schwachstellenscanner parametrisiert und ausgeführt. Bereits während der Analyse werden zumeist die ersten Systeme identifiziert, die für eine Detailanalyse in Frage kommen.

3.4.2 Tools und Techniken

Die Ergebnisse der Scans werden durch ein eigenes Tool kategorisiert, das sowohl die Vorbewertung durch die Schwachstellenscanner berücksichtigt, als auch eigene Bewertungskategorien, die auf im Einsatz gewonnenen Erfahrungen beruhen. Dabei wird immer das Ziel verfolgt, mit möglichst geringem Einsatz gute Ergebnisse zu erlangen. Solange ein System nicht explizit vom Kunden als zu testend benannt wurde, wird es während der Analyse dem Ranking entsprechend eingestuft. Unter Umständen wird es dann gar nicht getestet, denn nachdem die ersten Systeme erfolgreich angegriffen wurden, sind zumeist weitere Informationen verfügbar (beispielsweise Passworte von Administratoren), die ein neues Ranking erforderlich machen.

3.5 Detailanalysen Betriebssysteme

In diesem Kapitel wird das generelle Vorgehen bei der Detailanalyse einzelner Systeme beschrieben. Je nach zu betrachtendem System kann sich das Vorgehen ändern.

Innerhalb der einzelnen Abschnitte, die das Vorgehen beschreiben, wird, wenn notwendig, zwischen externem und lokalem Zugang zu dem System unterschieden.

In diesem Kapitel wird davon ausgegangen, dass ein direkter, nicht durch eine Firewall eingeschränkter Zugriff zum Zielsystem verfügbar ist.

3.5.1 Windows-basierte Systeme

Im Folgenden werden alle Microsoft Windows Systeme (Clients und Server) gemeinsam betrachtet.

3.5.1.1 Via Netz

Häufig geben Windows Systeme viele Informationen über sich selbst preis, ohne dass ein Systemdienst angegriffen werden muss. Diese Daten können mittels Anfragen an die Ports 135-139 und 445 abgefragt werden und bieten (je nach Systemkonfiguration) unter anderem Informationen über:

- den lokal angemeldeten Benutzer
- gestartete Dienste
- registrierte COM Objekte
- lokale Benutzer, lokale Gruppen
- Passwort-Einstellungen
- Freigaben
- Zugriffe auf Eventlogs

Diese Informationen können zusammen mit den Informationen aus dem Schwachstellenscan genutzt werden, um einen Angriff auf das System vorzubereiten. Dieser Angriff kann dann zunächst mit dem Ermitteln von Passwörtern zu den identifizierten Accounts starten oder, falls auf dem System vorhanden, konkrete Schwachstellen ausnutzen – wodurch ein viel effizienterer Angriff durchgeführt werden kann.

Noch immer laufen die meisten Dienste auf Windows Systemen mit den Berechtigungen des lokalen Systems. Ist ein solcher Dienst angreifbar und zum Absturz zu bringen, kann ein Zugriff mit den Berechtigungen des lokalen Systems auf dem gesamten Host erreicht werden. Dabei ist zu beachten, dass das lokale System über deutlich höhere Berechtigungen verfügt als der lokale Administrator. Ausgehend von einem Zugriff als lokales System (meistens als Kommandozeile, die via Netzwerk angebunden wird) können auf dem gesamten System eigene Prozesse gestartet werden. Diese Prozesse sind für den angemeldeten Benutzer nicht sichtbar, weil sie effektiv einem anderen Benutzer (eben dem lokalen System) zugeordnet sind.

Das häufigste Vorgehen bei einer erfolgreich ausgenutzten Schwachstelle ist, zunächst die Passwort-Hashes aller Benutzer auszulesen und zu kopieren. Mit geeigneten Mitteln können die Passwort-Hashes in reale Passwörter umgesetzt werden, die eine spätere Nutzung des Systems (auch nach eingespielten Updates) weiterhin erlauben. Zudem hat sich gezeigt, dass gerade Systemaccounts (lokale Administratoren, Antiviren-Programme, Softwareverteilung, etc.) auf vielen Systemen gleiche Passwörter verwenden. Ausgehend von einem schwachen System lassen sich dann weitere Systeme mit entsprechend hohen lokalen Berechtigungen leicht angreifen.

3.5.1.2 Lokaler Zugriff

Ist auf einem System lokaler Zugriff zulässig, können mit Systemberechtigungen die oben geschilderten Tätigkeiten ebenfalls durchgeführt werden. In den meisten Szenarien ist allerdings zunächst nur der Zugriff als normaler Benutzer erlaubt. Auch hier existieren mehrere Möglichkeiten, die eigenen Berechtigungen zu erhöhen bzw. auf Daten anderer Benutzer zuzugreifen.

Bei einem eingeschränkten Windows Betriebssystem sind die Verzeichnisse, die Anwender nicht sehen sollen, häufig mittels einer Funktion versteckt. Diese wird allerdings nicht von allen Anwendungen eingesetzt – wenn eine Anwendung genutzt wird, die versteckte Verzeichnisse ignoriert, kann auch auf diese Verzeichnisse zugegriffen werden. Hier liegen häufig Dokumente, die Anwender versehentlich dort gespeichert haben und dann nicht mehr lesen bzw. löschen konnten.

Zudem beherbergen Links auf Programme teilweise änderbare Ziele. Um erweiterte Rechte zu erlangen, kann einfach das Ziel eines Links geändert werden, indem beispielsweise eine Batch-Datei eingefügt wird, die unter den Rechten des jeweiligen Benutzers die Dateiberechtigungen für alle lesbar macht.

3.5.2 Unix-basierte Systeme

Bei Unix-basierten Systemen lässt sich das genaue Vorgehen zu Beginn weniger deutlich spezifizieren, da die bereitgestellten Dienste nicht so einheitlich sind wie bei Windows-basierten Systemen.

Bei Unix-basierten Systemen werden zunächst die laufenden Dienste identifiziert, über die dann versucht wird ins System vorzudringen. Das Vorgehen hängt davon ab, um welchen Dienst es sich handelt.

Bei Diensten mit einer Klartext-Authentisierung (wie telnet, ftp, mail, snmp) kann versucht werden (beispielsweise durch ARP-Poisoning Angriffe), die übertragenen Daten abzuhören und damit Kenntnis von Authentisierungsinformationen zu erlangen. Bei Anwendungen mit einer verschlüsselten Authentisierung könnte es zweckmäßiger sein, durch einen Man-in-the-Middle Angriff an entsprechende Informationen zu kommen. Zusätzlich lassen sich in beiden Varianten auch Brute-Force-Angriffe auf Authentisierungsinformationen starten, um eine gültige Benutzername/Passwort-Kombination herauszufinden.

Neben diesem generischen Vorgehen wird während der Analyse recherchiert, ob für den untersuchten Dienst bekannte Angriffe existieren. Diese werden dann in Absprache mit dem Auftraggeber ausgeführt.

3.6 Detailanalysen Funktionsserver

Neben der Analyse, die für einzelne Betriebssysteme typisch ist (siehe oben), gibt es auch Vorgehen, die für unterschiedliche Funktionsserver spezifisch sind. Diese Vorgehen werden im Folgenden kurz beschrieben. Bei einer Untersuchung werden sowohl die systemspezifischen Verfahren für das Betriebssystem als auch jene für die Funktion des Systems angewandt.

3.6.1 Datei-Server

Die offensichtliche Funktion eines Datei-Servers ist es, Daten in Form von einzelnen Datenobjekten (Dateien) für authentisierte Anwender bereitzustellen.

Die Analyse betrifft zum einen die Berechtigungen auf dem Server. Dazu wird auf alle Objekte zugegriffen, die unter den verschiedenen verfügbaren Berechtigungsstufen sichtbar sind. Insbesondere wird auch versucht, auf Objekte in untergeordneten Strukturen zuzugreifen, die von anderen Berechtigungsstufen her bekannt sind, für die aber auf dem übergeordneten Bereich keine Berechtigungen existieren (Bypass Traverse Checking).

Zum anderen erfolgt neben den oben beschriebenen Tests der reinen Zugreifbarkeit auch eine automatisierte Analyse hinsichtlich der Gefährdung der Daten[1]. Dies ist sinnvoll, da es

[1] Es muss jedoch berücksichtigt werden, dass die automatisierte Suche ohne Detailwissen über die jeweilige Umgebung nur unzureichend genau ist.

möglich ist, dass das Berechtigungsmanagement technische Probleme hat, oder auch (obwohl technisch korrekt) organisatorisch nicht angemessen umgesetzt ist. Zu den besonders kritischen Daten gehören aus Sicht der Analyse:

- Planungsdaten
- Personaldaten
- Skripte (mit Passworten)
- etc.

3.6.2 Terminal-Server

Die Analyse eines Terminal-Servers ist aufwendig, da die Anwendungen, die auf einem solchen betrieben werden, nicht auf einen Multi-User Betrieb in einer geschlossenen Umgebung ausgelegt sind. Die Anwendungen speichern teilweise die Konfigurationseinstellungen in zentralen Bereichen (beispielsweise %windir%), da sie für alle lokalen Anwender schreibbar sein müssen.

Die Analyse erfolgt im Allgemeinen mit den Berechtigungen eines lokalen Anwenders. Brute-Force Angriffe auf einen Terminal-Server sind zwar möglich, jedoch sehr zeitintensiv und bei einer gut installierten und beachteten Passwortrichtlinie meistens wenig Erfolg versprechend.

Ausgehend von einem Benutzer und den freigegebenen Anwendungen wird manuell versucht, aus dieser Umgebung auszubrechen um

- auf die Daten anderen Benutzer zuzugreifen,
- andere Programme als die für den Benutzer freigegebenen zu starten,
- eigene Programme hochzuladen und zu starten sowie
- das Netzwerk, in dem der Terminal-Server installiert ist, weiter zu untersuchen.

Zum Einsatz kommen hierbei Tools, die ohne Installation gestartet werden können, da die genutzten Zugänge auf dem Terminal-Server im Allgemeinen keine erweiterten Berechtigungen zulassen.

3.6.2.1 Web-Server / Portale

Bei der Analyse eines Web-Servers / eines Portals müssen neben dem zugrunde liegenden Betriebssystem auch noch die Web-Anwendung / das Portal betrachtet werden. Es hat sich gezeigt, dass neben den eigentlichen Informationen, die ein Portal bereitstellen soll, häufig auch noch viele andere Informationen (veraltete Versionen, zugreifbare Verzeichnisse, etc.) verfügbar sind. Daher wird in den Analysen neben den klassischen Angriffen wie Cross-Site-Scripting, SQL-Injection und Cookie Poisoning ein besonderes Augenmerk auf die Identifikation dieser nicht offensichtlich zugreifbaren Informationen gelegt.

Die Tests werden nach OWASP 4.0 durchgeführt. Dabei werden – in Abhängigkeit von der lokalen Berechtigung für die Anwendung – die folgenden Tätigkeiten realisiert:

- Betrachtung des Zielnetzes, in dem der Applikations-(Web-)Server erreichbar ist
- Identifikation der erreichbaren Schnittstellen auf dem Applikations-(Web-)Server
- Erfassung der zugreifbaren Informationen über den Applikations-Server
- Analyse der Serverstruktur
- Identifikation zugangsgeschützter Bereiche und Versuch, Passwörter zu ermitteln
- Analyse der Session-IDs
- Anmeldung am Server, Versuch der Erlangung erweiterter Berechtigungen
- Identifikation von Cross-Site-Scripting und Cross-Site-Tracing Potenzialen
- Identifikation von SQL-Injection Potenzialen
- Abhören von Authentisierungsinformationen
- Aufnahme der Dokumentenstruktur mit Spider- und Crawlingtools und manuell
- Analyse der Authentisierungsmechanismen (Übertragung der Passworte, Cookie-Generierung, etc.)
- Sammlung von Argumenten für einzelne URLs (GET)
- Sammlung von Argumenten, die via POST übermittelt werden
- Aufsuchen nicht angezeigter Verzeichnisstrukturen
- Aufsuchen von Helper Files (asp, cfm, css ,file ,htc ...)
- Aufspüren von JAVA Anwendungen (Klassen, Applets, Servlets ..)
- Suche und Analyse von HTML-Kommentaren
- Suche und Analyse von HTML-Formularen
- Suche von Query Strings
- Aufspüren von Backend-Verbindungen
- Eskalation der nutzbaren Berechtigungen
- Fuzzing-Angriffe, in denen Anwendungsparameter variiert werden
- Analyse der Kommunikationsbeziehungen
- Analyse der Berechtigungsstrukturen

Die Durchführung der Analyse erfolgt manuell mit der Unterstützung durch Tools, die schnell und effizient eine große Anzahl von Schwachstellen testen können.

Die Detailauswertung muss dann aber wieder manuell erfolgen, da nur eine solche Analyse auch Querbeziehungen zwischen unterschiedlichen Schwachstellen offenlegen kann. Dabei werden die übermittelten HTML-Seiten manuell verifiziert und auf logische Fehler, interne Datenflüsse und Kommentare hin untersucht. Identifizierte Cross-Site-Scripting oder SQL-Injektion-Angriffe werden manuell ausgenutzt, um das wirkliche Potenzial ausschöpfen zu können.

4 Weiterführende Analysen

Neben den standardmäßig angebotenen technischen Sicherheitsanalysen werden von Kunden immer häufiger auch gesonderte Analysen gewünscht. Diese werden im folgenden Kapitel beschrieben.

4.1 Analysen von mobilen Geräten

In einer durch globales Agieren geprägten Zeit kommt Smartphones eine wachsende Bedeutung zu, und die Einsatzszenarien werden immer komplexer. Denn die Hardware unterscheidet sich in ihrer Leistungsfähigkeit kaum noch von der herkömmlicher PCs. Außerdem bekommen User über Smartphones immer häufiger Zugang zu kritischen Unternehmensdaten und Diensten. Es ist deshalb wichtig, auch Smartphones in Sicherheitsüberprüfungen einzubeziehen.

4.1.1 Vorgehen

Generell lassen sich Audits von Smartphones in vier Kategorien einteilen:

1. Reverse-Engineering von Applikationen (Dekompilierung und Quellcodeanalyse)

2. Dateisystem- und Datenbankanalyse

3. Verhaltensanalyse von Applikationen auf dem Gerät/im Emulator

4. Netzwerkanalyse

Darüber hinaus können auch organisatorische Schwachstellen ausgenutzt werden. Zum Beispiel können eigene Appstores bereitgestellt werden, welche mit Schadcode infizierte Applikationen ausliefern.

4.1.2 Tools und Techniken

Das Reverse-Engineering von Applikationen ist ein wichtiger Bestandteil unserer Sicherheitsüberprüfungen, denn so können direkt Schwachstellen erkannt und nach Absprache mit dem Auftraggeber ausgenutzt werden.

Dabei gilt es zu unterscheiden, ob die Applikationen in einer Intermediate-Language vorliegen (beispielsweise Dex bei Android, Java und andere bei Blackberry, CLR bei Windows Phone, Javascript beim iPhone) oder ob es sich bei den Anwendungen um Bytecode handelt. Intermediate-Languages haben den Vorteil, dass sie sich relativ leicht in Hochsprache zurückwandeln (disassemblieren) lassen, wie es zum Beispiel von dem Werkzeug „Baksmali“ für

Android-Applikationen erledigt wird. Diese Hochsprachen sind für den Analysten relativ gut lesbar, so dass dieser direkt Schwachstellen erkennen kann. Darüber hinaus kann der Analyst solche Programme modifizieren und neu kompilieren, beispielsweise um Phishing-Applikationen zu entwickeln, oder um mit den Debuggern moderner Hochsprachen zu arbeiten.

Anwendungen, die im Bytecode vorliegen, sind schwerer zu analysieren, denn sie lassen sich in der Regel nur zu Assemblerprogrammen zurückübersetzen. Solche sind sehr „maschinennah“, so dass manuelle Analysen sehr aufwendig sind. Für Assemblerprogramme existieren allerdings Tools, die den Code automatisiert auf Schwachstellen untersuchen. Flawfinder beispielsweise sucht nach potenziell unsicheren Speicherzugriffen, die unter Umständen später vom Analysten für weiterführende Angriffe genutzt werden können.

Wichtige Hinweise können auch Dateien liefern, wobei zwischen Konfigurations-, Datenbank-, Anwendungs- und Temporär-Dateien unterschieden werden kann:

- Konfigurationsdateien beinhalten wichtige Hinweise über den Anwendungsrahmen, oft auch Authentisierungsinformationen.
- Datenbankdateien enthalten oft eine Vielzahl von Daten in strukturierter Form. Außerdem können sie ebenfalls Konfigurations- und Authentisierungsdaten zum Inhalt haben.
- Besondere Aufmerksamkeit erhalten auch gewöhnliche Dateien, denn vielen Firmen ist nicht bewusst, dass mobile Applikationen Kopien vertraulicher Dokumente speichern – häufig sogar unverschlüsselt.
- Auch Cachedateien können kritische Informationen enthalten. So legen einige Tastaturapplikationen Listen mit häufig gebrauchten Wörtern an, welche bei einer schlechten Implementierung der Keyboardapplikation sowie Applikationen von Drittherstellern Passwörter enthalten können.

Auch die Netzwerkanalyse ist ein wichtiger Punkt bei Sicherheitsaudits von Smartphones. Analog zu der Netzwerkanalyse von PCs und Serversystemen bietet sich hier an, den Netzwerkverkehr eines Smartphones über den PC des Analysten umzuleiten. Der Verkehr wird dann aufgezeichnet und später beispielsweise nach Authentisierungsinformationen durchsucht. Außerdem können Smartphone-Applikationen ähnlich wie Web-Applikationen getestet werden, unter anderem können SQL-Injektionen versucht werden. Im Falle von SSL-Verkehr werden spezielle MITM-Proxys eingesetzt.

Beim Testen von Smartphone-Applikationen werden außerdem weitere Eigenheiten der Smartphones berücksichtigt: So können den Anwendungen mit lokationsbasierten Authentifikationsentscheidungen beispielsweise falsche GPS-Koordinaten übermittelt werden.

Auch können – in Absprache mit dem Auftraggeber – entsprechend der Geräte Werkzeuge eingesetzt werden, die dem Analysten Root-Privilegien verschaffen.

4.2 Analyse aufgezeichneten Netzwerkverkehrs

Neben der Analyse einzelner Systeme im Netzverbund führt die Analyse des kompletten übertragenen Netzwerkverkehrs immer wieder zu Erkenntnissen, die mittels einer klassischen Systemanalyse nicht gewonnen werden können – gerade Malware kommuniziert auf betroffenen Systemen nicht über die Standard-Ports. Die meisten bösartigen Anwendungen sind durch einen Portscan nicht zu erkennen, da sie keine Dienste anbieten, sondern nur die Dienste anderer Systeme (beispielsweise Bot-Control-Server) nutzen. Durch die Analyse mehrtägiger Netzwerkmitschnitte kann die Kommunikation von Malware teilweise identifiziert und diagnostiziert werden.

4.2.1 Vorgehen

Zunächst werden ein oder mehrere Analysesysteme an geeigneten Plätzen im LAN des Auftraggebers platziert. Dabei ist darauf zu achten, dass möglichst alle Kommunikationswege, die das interne LAN verlassen, überwacht werden. Die Analysesysteme werden für ca. eine Woche im LAN belassen, bevor eine Auswertung der Daten erfolgt.

Zur Erstellung eines Überblicks über die aufgebauten Verbindungen werden die folgenden Informationen extrahiert:

- Network-Flows
- Zielsysteme
- Zielports
- Übermittelte URLs
- Verbindungen: internes System – Zielsystem – Zielport – Zeit

Zudem werden die gesammelten Daten durch ein IDS geschickt, wobei besonderes Augenmerk auf die Verbindungen gelegt wird, die das Netz verlassen.

4.2.2 Tools und Techniken

Es hat sich herausgestellt, dass viele der derzeit frei erhältlichen Tools zwar grundlegend die Analyse von Netzwerkdaten durchführen können, aber aus unterschiedlichen Gründen an großen Datenmengen (> 50GB) scheitern. Daher wurden viele Tools durch die secunet angepasst bzw. neu erstellt. Neben diesen eigenen Entwicklungen werden folgende Tools genutzt:

- Tcpdump/tshark
- argus
- afterglow
- Snort/Acid

Häufig lassen sich Malware-Anwendungen außer durch die oben genannten Tools auch durch besonderes Verhalten erkennen. Anhand der Verbindungsinformationen im Rahmen der Analyse wird bestimmt, welche Verbindungen in regelmäßigen Abständen aufgebaut werden. Diese sind zumindest beachtenswert und sollten mit dem Auftraggeber besprochen werden. Andere auffällige Verbindungen sind beispielsweise TCP-Verbindungen zu DNS-Servern. Das DNS-Protokoll nutzt üblicherweise das TCP-Protokoll nur zum Austausch von Zonen-Informationen. Malware hingegen kommuniziert teilweise über TCP via DNS oder über besondere Felder, die in den DNS-Paketen gewöhnlich nicht genutzt werden.

Anhand zusätzlicher IDS-Regeln und Hilfsprogramme lässt sich der gesammelte Datenstrom hinsichtlich solcher Anomalien durchforsten.

4.3 WLAN-Analysen

Praktisch zeitgleich zur verbreiteten Einführung von Funknetzen im privaten und kommerziellen Umfeld wurden auch effiziente Angriffe auf eben diese räumlich schwer kontrollierbaren Netze bekannt. Auch heute noch werden wenig oder nicht gesicherte WLANs in Unternehmen eingesetzt.

Zusätzlich bestehen auch Risiken durch WLANs, die zwar nicht vom eigenen Unternehmen betrieben werden, aber innerhalb der Geschäftsräume genutzt werden können oder schon einmal genutzt wurden. Ist ein fremdes WLAN innerhalb der eigenen Räumlichkeiten erkennbar, können die eigenen Mitarbeiter dieses WLAN nutzen, um an den etablierten Sicherheitsfunktionen des Unternehmen vorbei Zugriff ins Internet zu erlangen und dabei eine Netzkopplung schaffen, über die ein Angreifer ins interne LAN eindringen könnte.

Allein dadurch, dass ein Windows System über eine aktive WLAN-Karte verfügt und schon einmal ein ungesichertes WLAN genutzt hat, kann ein Risiko entstehen: Angreifer können über die vor Zeiten etablierte Verbindung zunächst auf das betroffene Windows System und danach in angeschlossene Netze vordringen.

Ziel der Analyse muss daher sein, zunächst einmal alle über Funknetze kommunizierenden Geräte zu identifizieren. Anschließend erfolgt eine Zuordnung der Geräte in die Klassen:

- fremder Access-Point
- eigener Access-Point
- eigenes System mit WLAN Karte
- sonstiges System

4.3.1 Vorgehen

Anhand der Tools werden die übertragenen Pakete analysiert und die identifizierten Systeme klassifiziert. Diese können in Absprache mit dem Auftraggeber angegriffen werden (beispielsweise zum Key-Recovery oder zum Angriff via bekannter Access Points). Dabei können die

theoretischen Angriffsmöglichkeiten verifiziert werden. Im Rahmen eines Angriffs wird dann versucht, den WEP/WPA Key zu berechnen (nur PSK Modus möglich). Alternativ kann ein Hotspot simuliert werden, mit dem sich ein System mit aktiver WLAN-Karte verbindet. Diese Verbindung kann dann genutzt werden, um das System anzugreifen.

4.3.2 Tools und Techniken

Die Analyse der zur Verfügung stehenden Systeme erfolgt toolgestützt. Zum Einsatz kommen unter anderem folgende Tools:

- Kismet
- Airo-Tools
- Hotspotter

4.4 War-Dialing

Auch wenn in der Zeit der günstigen DSL Anschlüsse, System-Telefonanlagen, Voice-Over-IP und VPN Zugänge die analogen und digitalen Modems immer mehr in den Hintergrund gedrängt werden, existieren immer noch Nischen, in denen einzelne Anschlüsse via Einwahl über Telefon-Modems erreichbar sind. Teilweise werden diese Modems zur automatischen Abrechnung von Energieversorgern genutzt, teilweise als Remote-Zugang von Wartungstechnikern. Im Rahmen eines War-Dialings werden in einem begrenzten Nummernblock automatisch analoge und digitale Modems identifiziert.

4.4.1 Vorgehen

Die Erstanalyse des abgesprochenen Nummernblocks wird durch ein automatisiertes Tool durchgeführt: Die Nummern des Blocks werden zufällig in einem mit dem Auftraggeber vereinbarten Zeitintervall (während der Geschäftszeiten, außerhalb der Geschäftszeiten oder rund um die Uhr) angewählt. Dabei werden sowohl digitale als auch analoge Modems erkannt. Die vom jeweiligen Endgerät übermittelten Zeichen werden protokolliert und zur weiteren Auswertung gespeichert.

Anhand der protokollierten Informationen der Endgeräte erfolgen manuelle Analysen und die Entwicklung von spezifischen Tools zur Kommunikation mit dem jeweiligen Endgerät. Je nach eingesetzter Software lassen sich die verwendeten Benutzernamen anhand einer Liste teilweise identifizieren. Ausgehend von diesen Listen werden dann Passwörter getestet, die einen Zugang ermöglichen können.

Für die Durchführung von War-Dialings ist im Allgemeinen mehr reale Zeit anzusetzen als bei IP-Analysen, da allein der Verbindungsaufbau – abhängig vom Endgerät – mehrere Minuten in Anspruch nehmen kann.

4.4.2 Tools und Techniken

Für War-Dialings werden ausschließlich selbst entwickelte Tools verwendet, die jeweils an die konkrete Umgebung angepasst werden.

4.5 Social Engineering

Beim Social Engineering werden explizit nichttechnische Methoden eingesetzt, um an vertrauliche Informationen zu gelangen. Im Folgenden werden Praktiken beschrieben, die schon erfolgreich eingesetzt wurden. Selbstverständlich werden die einzelnen Szenarien im konkreten Fall zusammen mit dem Auftraggeber verfeinert und speziell angepasst.

4.5.1 Remote Kontakt: Telefon

In diesem Szenario wird der Kontakt zum betroffenen Mitarbeiter über das Telefon hergestellt.

Ein Mitarbeiter des Auftragnehmers nimmt telefonischen Kontakt zu einer Zielperson beim Auftraggeber auf. In einem ersten Telefongespräch wird eine anonyme Befragung als Gesprächsgrund vorgeschoben. Im Rahmen dieser Befragung können bereits erste Informationen über die eingesetzten Systeme und Software-Produkte erlangt werden.

In einem zweiten Gespräch wird der Anruf eines internen Administrators vorgetäuscht. Dazu wird die abgehende Rufnummer des Auftragnehmer-Anschlusses auf eine interne Rufnummer des Auftraggebers geändert. Über diese Rufnummernänderung kann schon eine ‚Authentisierung' erreicht werden. Ausgehend von den im ersten Telefongespräch gewonnenen Informationen kann die Rolle eines Administrators gespielt werden. Als ‚Administrator' können weitere interne Informationen (beispielsweise verwendete IP-Adressen) erfragt werden.

4.5.2 Remote Kontakt: E-Mail

In diesem Szenario wird eine spezialisierte Phishing-E-Mail verfasst, die die Zielperson dazu motivieren soll, sich an einem vom Auftragnehmer kontrollierten Web-Server anzumelden.

Zunächst werden gültige E-Mail-Adressen im Adressbereich des Auftragnehmers identifiziert. Dazu wird insbesondere die Web-Präsenz des Auftraggebers zu Rate gezogen. Ausgehend von einer Liste mit gültigen IP-Adressen werden personalisierte E-Mails erzeugt, die die betroffenen Mitarbeiter beispielsweise dazu auffordern, sich mit ihrem normalen Benutzernamen und Passwort auf dem neuen ‚Unternehmensportal-Server' (einem Server im Internet, der durch den Auftragnehmer verwaltet wird) anzumelden. Die übertragenen Authentisierungsinformationen werden protokolliert und können für weitere Angriffe genutzt werden.

4.5.3 Indirekter Kontakt: Einschleusen von Medien

Normalerweise glaubt man nicht an etwas Gefährliches, wenn man hilfsbereit verloren geglaubte Dinge zurückgeben möchte oder wenn man interessante Werbegeschenke erhält. Die Praktik des indirekten Kontakts setzt genau hier an, um einen speziellen Trojaner im Unternehmen einzuschleusen.

Ziel: Ein vom Auftragnehmer vorbereitetes Medium soll in die IT-Systeme des Auftraggebers eingeschleust und dort ausgeführt werden.

Variante 1: Es werden Werbebriefe erstellt, die jeweils einen USB-Stick enthalten, auf dem offenkundig ein Prospekt des Werbenden hinterlegt ist.

Variante 2: Auf und vor dem Gelände des Auftragnehmers werden gezielt USB-Sticks ‚verloren'. Der Finder wird einen gefundenen USB-Stick vermutlich in den eigenen USB-Anschluss stecken, um den ursprünglichen Besitzer zu identifizieren…

Anmerkung:
Der Trojaner wird von Anti-Virenprogrammen nicht erkannt, da er speziell für diesen Auftrag geschaffen wird. Er ist so verfasst, dass er:

- sich nicht selbsttätig verbreitet (er wird nur ausgeführt, wenn der USB-Stick in einen Computer eingesteckt wird)
- sich nicht auf andere Computersysteme überträgt
- keine vertraulichen Informationen liest, ändert oder löscht
- sich selbst ab einem bestimmten Datum spurlos löscht
- keine Rückschlüsse auf den Auftragnehmer oder den Auftraggeber zulässt

5 Organisatorische Analysen

Organisatorische Analysen finden als Basisanalysen für Informationssicherheit in der Regel in Form gelenkter Interviews statt. Anhand mehrerer Fragebögen werden die zentralen Bereiche der organisatorischen Informationssicherheit beleuchtet. Dabei werden die Antworten der Mitarbeiter hinterfragt, plausibilisiert und stichpunktartig verifiziert. Die einzelnen Fragen werden nach secunet Best Practice oder in Zusammenarbeit mit dem Auftraggeber in Abhängigkeit von unterschiedlichen Parametern (z. B. Geltungsbereich (Scope), Schutzbedarf, etc.) gewichtet und ausgewertet.

Die Analyse beinhaltet folgende Bereiche:

- Organisation: Allgemeine Organisation, Personal, Vertragsbeziehungen und Outsourcing
- Informationssicherheit: Informationssicherheitsorganisation, Risikomanagement, Notfallmanagement, Mitarbeitersensibilisierung
- Physische Sicherheit: Allgemeine Faktoren, Zutrittsschutz und Überwachung, Energieversorgung, Klimatechnik, Brandschutz
- IT-Service Management: Incident Management, Problem Management, Release und Deployment Management, sonstige IT-Service Management Themen
- IT-Sicherheit: Berechtigungsvergabe, Client-Sicherheit, Server-Sicherheit, Sicherer Betrieb, Netzwerksicherheit, mobile Endgeräte, Virenschutz, Email- und Internetnutzung, Datensicherung
- Compliance: branchenspezifische und allgemeine gesetzliche Vorgaben (z. B. BDSG)

6 Dokumentation der Analysen

Die secunet AG schließt jede Sicherheitsprüfung mit einer für den Auftraggeber transparenten Dokumentation ab, die das bestimmte Sicherheitsniveau der eingesetzten Systeme, die identifizierten Schwachstellen sowie die empfohlenen Maßnahmen zur Behebung der Schwachstellen beinhaltet.

6.1 Aufbau einer Dokumentation

Die Beschreibung setzt sich aus den drei Komponenten Schwachstelle {S}, Risiko {R} und Maßnahme {M} mit einer zugehörigen Nummer zusammen.

Schwachstelle
Hier wird die identifizierte Schwachstelle beschrieben. Dabei werden Bedrohungen der **Integrität** (können die Daten unberechtigt verändert werden?), der **Verfügbarkeit** (kann die Erreichbarkeit eines Systems/Dienstes eingeschränkt werden?) und der **Vertraulichkeit** (kann ein Unberechtigter auf die Daten lesend zugreifen?) unterschieden. Pro Kategorie werden die Klassen **hoch**, **mittel** und **niedrig** unterschieden, die angeben, wie kritisch die jeweilige Bedrohung eingeschätzt wird.

Risiko
Dieser Bereich stellt das Risiko dar, das durch das Vorhandensein der Schwachstelle hervorgerufen wird. Auch hier werden die Klassen **hoch**, **mittel** und **niedrig** unterschieden.

Maßnahme
Der dritte Teil der Dokumentation beschreibt schließlich Maßnahmen, die getroffen werden sollten, um die Schwachstellen zu schließen. Die Maßnahmen stellen Empfehlungen dar, die in Zusammenarbeit mit den IT-Mitarbeitern verfeinert werden müssen.

Die Priorisierung der Maßnahmen leitet sich direkt aus der Gefährdung der Schwachstellen und dem identifizierten Risiko ab und erfolgt anhand der Kategorien **zeitnah**, **kurzfristig**, **mittelfristig** und **langfristig**.

6.2 Struktur & Klassifizierungen

Die von der secunet vorgelegten Dokumentationen der Sicherheitsanalysen basieren auf den Richtlinien des OSSTMM[2]-Standards. Jeweils zu Beginn eines Kapitels sind die durchführenden Mitarbeiter der Analyse sowie der Analysezeitraum dokumentiert. Bei Bedarf werden diese Informationen für einzelne Unterkapitel noch einmal präzisiert. Die Dokumentationsberichte beinhalten alle getesteten Bereiche und Server und beziehen sich, soweit möglich, auf eine Überprüfung aller relevanten OSI-Layer im getesteten Netzwerk.

[2] OSSTMM steht für Open Source Security Testing Methodology Manual. Dieses Dokument wird vom Institute for Security and Open Methodologies (ISECOM) erstellt und beschreibt unter anderem, wie Sicherheitsaudits durchgeführt werden sollten.

Für die Überprüfung der abstrakteren OSI-Layer (Anwendungs-, Darstellungs- und Sitzungsschicht) erfolgen die einzelnen Schritte der Analyse sowie deren Klassifizierung nach OWASP (Open Web Application Security Project) in der Version 4.0. Diese Version befindet sich zwar noch im Draft-Zustand, wird allerdings genutzt, da einige der aktuellen Angriffsvektoren in dem publizierten Standard OWASP 3.0 aus dem Jahre 2008 noch nicht enthalten sind. Da OWASP 4.0 alle Angriffsvektoren von OWASP 3.0 umfasst und diese nur um zusätzliche Vektoren erweitert, werden trotz des Draft-Zustandes des neuen Standards keine Angriffsvektoren des bisherigen Standards vernachlässigt.

6.3 Abgrenzung

Bei einer technischen Sicherheitsanalyse oder einem Penetrationstest handelt es sich naturgemäß um eine stichprobenartige Analyse, in der versucht wird, mit einem endlichen Aufwand möglichst viele Schwachstellen innerhalb eines Untersuchungsobjektes zu finden.

Im Normalfall lässt sich nur ein Teil der gefundenen Systemeigenschaften klar als Schwachstelle einstufen. Der andere Teil benötigt eine weitergehende Überprüfung, inwieweit die identifizierten Eigenschaften eines Systems Funktionen sind, die als Anforderung implementiert wurden und inwieweit durch diese Implementierung Schwachstellen erzeugt wurden, die mit einer alternativen Implementierung vermieden werden können.

Durch die hier entstehende Menge der Kombinationsmöglichkeiten muss für den Rahmen des zur Verfügung stehenden Zeitkontingentes eine Abwägung zwischen der Menge der zu bewertenden Eigenschaften und der Tiefe der durchzuführenden Untersuchung getroffen werden.

Weiterhin muss eine technische Sicherheitsanalyse immer als **Betrachtung** zu einem **Stichtag** aufgefasst werden. Die zu diesem Tag bekannten Schwachstellen und Angriffstechniken werden genutzt. **Aussagen über die Zukunft lassen sich jedoch nicht treffen.** Ein System, bei dem keine Schwachstelle gefunden wurde, kann bereits einen Tag später durch eine neu entdeckte Schwachstelle angreifbar werden. Zum Beispiel können auch kleinste Änderungen an den Systemeinstellungen positive oder negative Auswirkungen auf die Systemsicherheit haben.

Allerdings lassen sich bei vielen Analysen Trends identifizieren: Systeme, auf denen Schwachstellen identifiziert wurden, die bereits seit vielen Monaten bekannt sind, werden offenbar nicht regelmäßig aktualisiert. Ändert sich an dem Verhalten der Systembetreuer nichts, wird dieser Zustand vermutlich auch in Zukunft erhalten bleiben und das System (auch wenn direkt nach der technischen Sicherheitsanalyse ein komplettes Update erfolgt) zukünftig wieder zum Sicherheitsrisiko werden.

Im Rahmen der aus den identifizierten Schwachstellen abgeleiteten Maßnahmen ist darauf zu achten, dass diese Maßnahmen nicht nur vorübergehend Schwachstellen beheben, sondern zusätzlich auch langfristig zu warten und zu überwachen sind.

7 Fazit

Technische Sicherheitsanalysen sind schon seit Jahren ein probates Mittel, um mit wenig Aufwand Systeme, Systemverbünde und Netzwerke zu überprüfen. Durch die kleinen Budgets, die für die Durchführung einer technischen Sicherheitsanalyse benötigt werden und die Variantenbreite lassen sich Analysen für jeden Zweck zusammenstellen.

Als Ergebnis erhält ein Auftraggeber einen Maßnahmenkatalog von Schwachstellen, die behoben werden sollten. Ist diese Liste abgearbeitet, lassen sich viele typische Angriffe nicht mehr durchführen. Dies schützt die Mitarbeiter vor unbeabsichtigten Fehlern und macht Industriespionen die „Arbeit“ gleichzeitig deutlich schwerer.

Neben den gefundenen Schwachstellen selbst (deren Behebung durch den vorgelegten Report beschrieben und deren Umsetzung priorisiert wird) kann eine technische Sicherheitsanalyse aber auch Hinweise auf die Ursachen des Auftretens der Schwachstelle geben. Diese Ursachen lassen sich zumeist in den Bereichen

- mangelnde Ressourcen für das Testen und Aktualisieren von Systemen,
- fehlende Dokumentation,
- nicht ausreichende Kenntnis über aktuelle Angriffsstrategien,
- Konfigurationsfehler und
- Programmierfehler

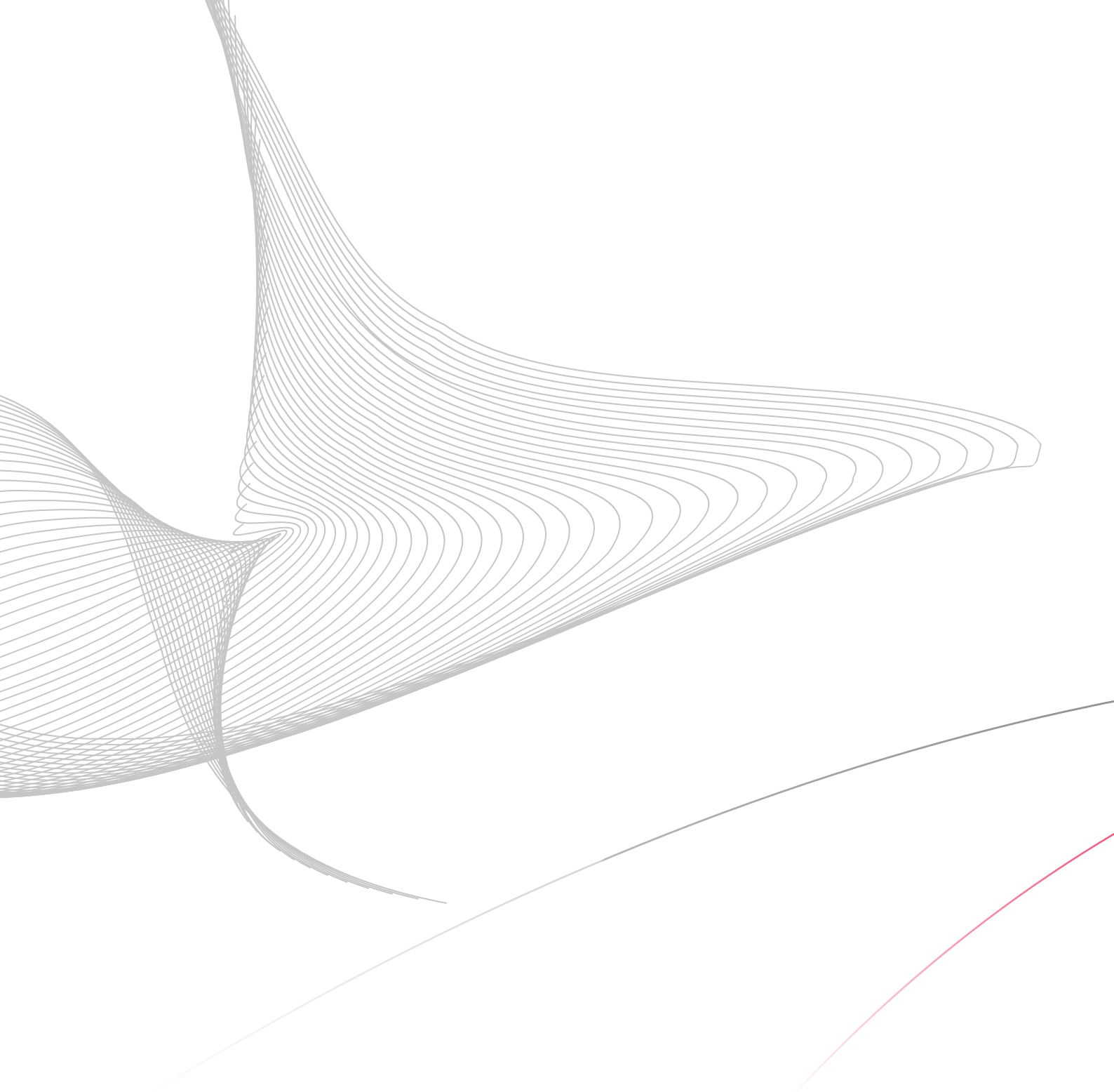
finden. Im Nachgang können dann basierend auf den Ergebnissen einer durchgeführten technischen Sicherheitsanalyse interne Prozesse geschaffen und angepasst werden, die verhindern, dass vergleichbare Schwachstellen erneut auftreten. Damit kann eine technische Sicherheitsanalyse nicht nur für eine punktuelle und temporäre Steigerung der Systemsicherheit sorgen, sondern als Teil einer Sicherheitspolitik zur Nachhaltigkeit der IT-Sicherheit beitragen.

Dieser wünschenswerte Effekt zeigt sich insbesondere bei Kunden, die technische Sicherheitsanalysen als Teil der Produktentwicklung betrachtet. Bei mehreren Kunden konnte die secunet zeigen, dass sich die Qualität der intern entwickelten Anwendungen messbar gesteigert hat, nachdem die Pflicht zur Durchführung einer technischen Sicherheitsanalyse in den Abnahmeprozess integriert wurde.

Dieser positive Effekt kann dann auch als return of security invest bezeichnet werden und stellt dar, welche positiven Auswirkungen der Einsatz von (unter anderem) technischen Sicherheitsanalysen bringen kann.

Weitere Informationen:

www.secunet.com/pentest



secunet

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Tel: +49-201-54 54-0
Fax: +49-201-54 54-1000
E-Mail: info@secunet.com
www.secunet.com