

## Whitepaper

# Durchführung und Gestaltungsmöglichkeiten von Penetrationstests

Stand: 11.05.2011

**SySS GmbH**  
<http://www.SySS.de>  
Wohlboldstraße 8  
72072 Tübingen  
Tel.: 07071-407856-0  
Fax: 07071-407856-19  
E-Mail: [info@SySS.de](mailto:info@SySS.de)

### **Autoren:**

Sebastian Schreiber    [Sebastian.Schreiber@SySS.de](mailto:Sebastian.Schreiber@SySS.de)  
Stefan Arbeiter        [Stefan.Arbeiter@SySS.de](mailto:Stefan.Arbeiter@SySS.de)

### **Qualitätssicherung:**

Micha Borrmann (Modul LAN/WAN)    [Micha.Borrmann@SySS.de](mailto:Micha.Borrmann@SySS.de)  
Christoph Bott (Modul WLAN)        [Christoph.Bott@SySS.de](mailto:Christoph.Bott@SySS.de)  
Katrin Heinrich (Modul WEBAPP)     [Katrin.Heinrich@SySS.de](mailto:Katrin.Heinrich@SySS.de)



**Über den Geschäftsführer**

- 1993-1999 Studium der Informatik, Physik, Mathematik und BWL an der Eberhard-Karls-Universität Tübingen
- 1996-1998 Mitarbeiter bei Hewlett-Packard
- 1996 MicroGold (USA)
- 1998-heute Geschäftsführer der SySS GmbH (Sicherheitstests bei einer Vielzahl von Unternehmen)
- Zahlreiche Veröffentlichungen, Vorträge im In- und Ausland; Mitherausgeber der IT-Sicherheit und Datenschutz

Sebastian Schreiber

## Inhalt:

1. Zusammenfassung .....	3
2. Gestaltungsmöglichkeiten .....	3
2.1. Testgegenstand und Testabdeckung .....	4
2.2. Testtiefe .....	5
2.3. Testfrequenz .....	5
2.4. Wissensstand bei Sicherheitstests .....	6
2.5. Testperspektive .....	7
2.6. Aggressivität des Tests .....	8
2.7. Risiken bei Sicherheitstests .....	10
2.8. Angekündigte oder unangekündigte Prüfungen .....	11
2.9. Social Engineering .....	12
2.10. Verdeckte oder offensichtliche Tests .....	13
3. Projektmodule .....	14
3.1. Kick-Off: KICKOFF .....	14
3.2. Perimetererkennung: PERIM .....	15
3.3. Analyse aus dem Internet: INTERNET .....	16
3.4. Prüfung von Web-Applikationen: WEBAPP .....	19
3.5. Sicherheitstest im internen Netz: LAN/WAN .....	29
3.6. WLAN-Test: WLAN .....	34
3.7. Produkt-/Labortests: PRODUCT .....	36
3.8. Dokumentation: DOCU .....	38
3.9. Präsentations-Workshop: PRES .....	39
3.10. Nachtest: RETEST .....	40
4. Besondere Prüfungen .....	41
4.1. Test von Systemen Dritter (Dienstleister, Lieferanten u.a.) .....	41
4.2. Forensische Analysen: FORENSIC .....	42
4.3. Prüfung organisatorischer Vorgaben: REVIEW .....	44
4.4. Individuelles Anliegen: INDIVIDUAL .....	45
5. Grundlagen des Sicherheitstests .....	45
5.1. Grenzen von Sicherheitstests .....	45
5.2. Abgrenzung von Sicherheitstests zu anderen Prüfungen .....	46
5.3. Zehn Tipps von Sebastian Schreiber .....	46
6. Über die SySS GmbH .....	47
6.1. Firmengeschichte: .....	47
6.2. Besondere Vorgehensweise: .....	48
6.3. Werkzeuge: .....	49
6.4. Grundlegende Ethik für Penetrationstester .....	50
6.5. Beschreibung der technischen Risiken bei Tests .....	52
6.6. Veröffentlichungen der SySS GmbH (Auswahl) .....	54

## 1. Zusammenfassung

Dieser Leitfaden beruht auf der über zehnjährigen Erfahrung der SySS GmbH mit der Durchführung von Sicherheitstests, sowohl bei großen multinationalen als auch bei traditionellen mittelständischen Unternehmen. Er basiert außerdem auf den praktischen Erfahrungen unserer Consultants und auf der intensiven Kommunikation mit unseren Kunden.

Sicherheits- oder Penetrationstests versteht die SySS GmbH als aktive Qualitätskontrolle der IT-Sicherheit. Innerhalb dieses Bereichs liegt ihre Kernkompetenz im Test von klassischen Netzen, Webapplikationen und WLANs.

Dieser Text unterstützt Sie dabei, die richtigen Testgegenstände und das dazu aus dem Angebot der SySS GmbH passende Testverfahren auszuwählen. Zudem wird dargestellt, welche Voraussetzungen nötig sind, damit ein Test effizient und im positiven Sinne erfolgreich durchgeführt werden kann.

Insbesondere wird gezeigt, welche Entscheidungen und Maßnahmen erforderlich sind, damit der Test auch intern in Ihrem Unternehmen als eine besonders positive Dienstleistung wahrgenommen wird.

## 2. Gestaltungsmöglichkeiten

Allein aufgrund des Gegenstandes, nämlich IT-Systemen unterschiedlichster Art, können Sicherheitstests nicht nach einem festen, standardisierten Verfahren ablaufen. Sie können – und müssen – flexibel gestaltet werden. Diese Gestaltung ist von mehreren Faktoren abhängig, unter anderem von

- der Perspektive, aus der der Test durchgeführt wird (siehe Testperspektive, Seite 7)
- dem Umgang mit *DoS (Denial of Service)*-Potentialen (siehe Aggressivität, Seite 8)
- der internen Koordination des Testablaufs (siehe „Angekündigte/Unangekündigte Prüfungen“, Seite 10)
- den zu testenden Systemen bzw. Anwendungen (siehe Testgegenstand, Seite 4)
- den möglichen Schwerpunkten (siehe Testtiefe, Seite 5)

- der Regelmäßigkeit der Tests (siehe Testfrequenz, Seite 5),
- den Besonderheiten beim Testverfahren (siehe verdeckte oder offensichtliche Tests, Seite 12)
- den gewählten Testmodulen (siehe Projektmodule, Seite 14)
- und dem zur Verfügung stehenden Budget.

## 2.1. Testgegenstand und Testabdeckung

Sowohl bei externen (Modul INTERNET) als auch bei internen Tests (Modul LAN/WAN) sind die Testgegenstände Systeme und daher konkret deren IP-Adressen. Aus der Gesamtheit der IP-Adressen wählt der Kunde entweder eine repräsentative Stichprobe aus oder es werden alle getestet.

Bei dem Test von Webapplikationen (Modul WEBAPP) ist der Testgegenstand eine webbasierte Anwendung bzw. deren Funktionalität.

Bei der Untersuchung von WLANs (Wireless LANs) ist der Testgegenstand wiederum das WLAN an einem Standort des Kunden sowie daraus ausgewählte Clients. Die Testabdeckung beschreibt hier zum Beispiel die Größe des zu untersuchenden Campus oder die Anzahl der zu prüfenden Gebäude.

Der Testgegenstand und die Testbreite werden bei der Angebotserstellung berücksichtigt; an dieser Stelle wird auch der Zeitbedarf kalkuliert. Aufgrund der Vielfalt an Systemen und Anwendungen, die in allen Fällen zum Einsatz kommen können, sind pauschale Aussagen schwierig. Wir empfehlen Ihnen daher, den Testgegenstand vorab direkt mit uns zu besprechen.

Im Allgemeinen wird – insbesondere bei großen Unternehmen – im Rahmen eines Tests nicht das gesamte interne oder externe Netz geprüft, sondern eine sinnvolle Auswahl getroffen. Als Sonderform ist es möglich, dass die SySS GmbH aus einem oder mehreren Netzen selbständig Stichproben auswählt.

Stellt entweder der Kunde oder die SySS GmbH während eines Tests fest, dass Änderungen sinnvoll sein könnten, so sind Anpassungen, die die Testdauer insgesamt nicht verändern, unbürokratisch möglich. Sie werden in direkter Absprache zwischen dem durchführenden Consultant und dem Ansprechpartner des Kunden vorgenommen.

## 2.2. Testtiefe

Die Testtiefe ergibt sich automatisch aus dem gewählten Testgegenstand und der zur Verfügung stehenden Zeit. Ist ein Testziel beispielsweise die Überblicksgewinnung über eine große Anzahl von Systemen in vergleichsweise kurzer Zeit, so ist die Testtiefe des einzelnen Systems niedrig und die Suche nach sehr hohen Risikopotentialen hat Priorität. Steht dagegen viel Zeit für wenige Systeme zur Verfügung, so können beispielsweise Fehlkonfigurationen erfasst werden, von denen kein direktes Sicherheitsrisiko ausgeht.

Die Schwerpunktsetzung bei der Untersuchung des im Angebot definierten Testgegenstandes wird im Kick-Off besprochen. Das generelle Ziel ist, innerhalb des Testzeitfensters festzustellen, wie das aktuelle Sicherheitsniveau des Testgegenstandes aussieht und von welchen Sicherheitslücken das größte Risiko ausgeht. In der Regel wird der durchführende Consultant mehr Aufwand in den Nachweis von Sicherheitslücken investieren, die ein Eindringen Dritter ermöglichen, als in die detaillierte Untersuchung von Fehlern, die nur ein minimales Risiko darstellen.

Endgültiges Ziel ist, ein möglichst umfassendes Gesamtbild über den Sicherheitszustand des Testgegenstandes zu erstellen, Risiken klar zu benennen und Vorschläge zur Behebung derselben zu unterbreiten. Dies alles geschieht in der Form eines Berichtes (Modul DOCU).

Wenn die Notwendigkeit erkannt wird, während des Tests die Schwerpunktsetzung oder Testtiefe zu ändern, so ist auch dies im direkten Gespräch zwischen Consultant und Ansprechpartner möglich. Da Sicherheitstests keine linearen Abläufe sind, bietet die SySS GmbH hier die nötige Flexibilität.

## 2.3. Testfrequenz

Sicherheitstests entfalten ihre maximale Wirkung auf den Sicherheitsprozess nicht, wenn sie nur einmalig stattfinden – denn die Maßnahmen, die nach einem Test zur Behebung festgestellter Sicherheitslücken durchgeführt werden, sollten für die Mitarbeiter oder Dienstleister zur Routine werden.

Für nachhaltige Ergebnisse sollte der Sicherheitstest vollständig in den Sicherheitsprozess integriert und turnusmäßig durchgeführt werden. Unternehmen, die einen hohen Wert auf die IT-Sicherheit legen, konzipieren Testpläne, die zwei bis drei Jahre in die Zukunft reichen:

	Q2 2010	Q3 2010	Q4 2010	Q1 2011	Q2 2011	Q3 2011	Q4 2011
Sicherheitstest der Systeme im Internet (Modul INTERNET)		X			X		
Untersuchung der Webapplikationen (Modul WEBAPP)			X			X	
Interner Penetrationstest (Modul LAN/WAN)				X			X
WLAN-Test (Modul WLAN)	X				X		

Dabei muss der permanente Wandel von IT-Netzen und Anwendungen berücksichtigt werden. Die Planung sollte etwa halbjährlich überdacht und aktualisiert werden. Des Weiteren kann für den jeweiligen Test der Testgegenstand so gewählt werden, dass sich der Nutzen maximiert und keine Routine im negativen Sinn (Gleichgültigkeit gegenüber den Testergebnissen) eintritt. Nur mit einem Testplan, der langfristig angelegt ist, lassen sich auftretende Schwachpunkte identifizieren und ein professionelles Qualitätsmanagement nachweisen.

## 2.4. Wissensstand bei Sicherheitstests

Bei einem Sicherheitstest wird sowohl eine bestimmte Perspektive eingenommen (siehe Testperspektive) als auch von einem bestimmten Wissensstand des potentiellen Angreifers ausgegangen. Die SySS GmbH orientiert sich bei Bedarf grob an dem Blackbox-, Whitebox- und Greybox- Modell.

### „Blackbox“-Modell:

Bei diesem Modell werden durch den Kunden nur minimale Informationen über den Testgegenstand übermittelt.

Ein „Blackbox“-Test darf dabei aber keinesfalls als Test missverstanden werden, bei dem keinerlei Informationsfluss zwischen Tester und Kunden stattfindet und Ziele völlig selbständig gewählt und geprüft werden. Rechtliche Gegebenheiten erlauben das Testen von fremden Systemen ohne ausdrückliche Erlaubnis des tatsächlichen Betreibers nicht.

Vor einer Prüfung muss zudem stets verifiziert werden, ob ein Test des Systems oder des Netzes aus organisatorischen und technischen Gesichtspunkten sinnvoll ist.

Falls sich die Auswahl aufwendig gestaltet, kann eine Perimetererkennung durchgeführt werden (Modul PERIM). Dabei identifiziert die SySS GmbH Testziele möglichst selbständig. Die Ergebnisse und die Stichprobenauswahl werden mit dem Kunden besprochen, der die Testfreigabe erteilt und die nötigen Genehmigungen beschafft.

#### **„Whitebox“-Modell:**

Dabei werden umfangreiche Informationen über den Testgegenstand übermittelt. In der Regel ist die hier übliche Informationsfülle für die Durchführung eines Sicherheitstests im Rahmen des Moduls INTERNET nicht erforderlich.

#### **„Greybox“-Modell:**

Sicherheitstests der SySS GmbH fallen in der Regel in diese Kategorie. Dabei werden von dem Kunden exakt die Informationen zur Verfügung gestellt, die zur effizienten Durchführung eines Sicherheitstests nötig sind. Falls höherer Informationsbedarf besteht, werden Rückfragen an einen Ansprechpartner des Kunden gestellt.

Die Informationen, die für das jeweilige Testmodul nötig sind, werden jeweils unter „Mitwirkung des Kunden“ beim entsprechenden Modul genannt.

Nach der langjährigen Erfahrung der SySS GmbH ist dies die effizienteste Methode.

## **2.5. Testperspektive**

Die unterschiedlichen Positionen, die ein potentieller Angreifer einnehmen kann, werden notwendigerweise durch unterschiedliche Testabläufe abgedeckt.

Zum einen kann geprüft werden, welche Infrastruktur des Kunden überhaupt aus dem Internet erreichbar ist. Damit wird das Risiko eingeschätzt, von dort aus Ziel von Angriffen zu werden (Modul PERIM). Dies kann auch als Inventarisierungsmaßnahme verstanden werden.

Soll geprüft werden, welches Risiko konkret von im Internet erreichbaren Systemen durch nicht-privilegierte Nutzer ausgeht, werden diese Systeme einem externen Test unterzogen (Modul INTERNET).

Davon zu unterscheiden ist der Test von Web-Applikationen. Er findet primär aus der Perspektive von regulären Nutzern (im Gegensatz zu nicht angemeldeten Besuchern) einer webbasierten Anwendung statt, auch wenn er vom Internet aus durchgeführt wird (Modul WEBAPP). Der Test kann zusätzlich auch die Perspektive des unangemeldeten Besuchers einnehmen.

Der Sicherheitstest im internen Netz (Modul LAN/WAN) prüft das (Firmen-)Netz aus der Perspektive des Innentäters. Zwangsläufig findet er daher am Objekt statt. Bei einem internen Test sind in der Regel sehr viele Systeme, die zudem auch viele Dienste anbieten, erreichbar. Daher muss die Art der Durchführung von der etwas abweichen, die bei externen Tests angewandt wird. Dies umfasst unter anderem eine Konzentration auf die Feststellung von schwerwiegenden Sicherheitslücken, die leicht ausgenutzt werden können.

Bei den Sicherheitstests von WLANs (Modul WLAN) wird zunächst einmal die Perspektive eines Angreifers in der Reichweite einer WLAN-Antenne eingenommen. Hier wird geprüft, ob z. B. die unberechtigte Nutzung eines Netzes möglich ist oder bestehende Verbindungen von Teilnehmern kompromittiert werden können. Ebenso wie der interne muss der WLAN-Test zwangsläufig vor Ort stattfinden.

## **2.6. Aggressivität des Tests**

Hier kommt *DoS (Denial of Service)*-Potentialen besondere Bedeutung zu. Zum einen können diese durch Fehler in Diensten selbst auftreten, zum anderen durch Fehlkonfigurationen.

Generell ist es nicht das Ziel eines Sicherheitstests, Systeme oder Anwendungen außer Kraft zu setzen, sondern derartige Gefahrenquellen aufzuzeigen.

Folgendes Vorgehen hat sich bei der Erkennung von *DoS*-Potentialen besonders bewährt: Wird ein solches gefunden, kontaktieren wir zuerst den Ansprechpartner des Kunden. Im direkten Gespräch wird entschieden, ob die SySS GmbH den tatsächlichen Nachweis führen (also die Störung auslösen) soll oder nicht. Das Ausnutzen eines *DoS*-Potentialen kann sinnvoll sein, wenn der Kunde ein klares Signal wünscht, dass an einem bestimmten System Änderungen (Wartung, Abschottung oder gar Ersatz) nötig sind.

Um die Auswirkungen der Störungen, die durch den Nachweis eines *DoS*-Potentialen entstehen, zu verringern, können folgende Maßnahmen getroffen werden:

- Test zu Zeiten niedriger Last bzw. außerhalb der Hauptnutzzeit,
- Nachweis an Testsystemen (falls verfügbar),
- falls das Potential in vielen Fällen festgestellt wird, Wahl von Stichproben.

Zusätzlich muss bei der Durchführung ein Systemverantwortlicher erreichbar sein.

Tests, deren Ziel es ist, durch den Verbrauch von Bandbreite Netze lahmzulegen, führt die SySS GmbH nicht durch. Das Risiko durch derartige Angriffe besteht immer und kann durch die Betrachtung der zur Verfügung stehenden Bandbreite jederzeit ermittelt werden.

Da es sich bei einem Sicherheitstest um eine aktive Kontrolle handelt, kann nie völlig ausgeschlossen werden, dass die zu testenden Systeme beeinträchtigt werden. Beeinträchtigungen können sowohl bei Funktionen einzelner Dienste, dem getesteten Dienst selbst oder dem gesamten getesteten System auftreten.

Insbesondere bei dem Test von Webapplikationen wird normalerweise nicht von *DoS*-Potentialen ausgegangen. Da aber während eines Tests Abfragen an die Datenbank gestellt werden können, die reguläre Anwender nicht erzeugen, bestehen diese Risiken auch hier. Oft ist es schwer, derartige Probleme vorherzusehen. Gibt es jedoch klare Indikatoren dafür, kann wie oben dargestellt vorgegangen werden.

Ein Sicherheitstest, der keinerlei Risiken birgt, ist nicht möglich.

Zwei Gründe sind nach der Erfahrung der SySS GmbH für *DoS* bei Sicherheitstests verantwortlich: Zum einen Systeme oder Anwendungen, die auch mit der nur moderaten Last eines Tests nicht umgehen können und zum anderen sehr alte und ungepflegte Dienste.

Generell sollte bei der Vorbesprechung (Kick-Off) angesprochen werden, ob und wie alte oder sehr alte Systeme getestet werden (z. B. mit Patchstand Jahr 2006 oder älter), oder ob Lastprobleme ohnehin auftreten. Um letzteres Problem zu umgehen, kann auch vereinbart werden, bestimmte Prüfungen außerhalb von Spitzenlastzeiten durchzuführen.

## 2.7. Risiken bei Sicherheitstests

Penetrationstests gehen immer mit einem unvermeidbaren Risiko einher, welches sich aber nur punktuell von Funktions-, Last- und Verbindungstests unterscheidet. In gleicher Weise wie bei derartigen Tests muss bei einer Sicherheitsüberprüfung mit einem bestimmten Datenvolumen gerechnet werden, welches die beteiligten Systeme wie im normalen Betrieb abarbeiten müssen.

Der Hauptunterschied zu anderen Testverfahren ist, dass bei einem Sicherheitstest verschiedene Dienste mit Anfragen konfrontiert werden, die im Alltag nicht auftreten.

Dies ist exakt das grundlegende Vorgehen zum Erkennen von Sicherheitsdefiziten aller Art, von dem nicht abgewichen werden kann, es sei denn, man möchte auf technische Maßnahmen vollständig verzichten.

Um also möglichst viele Risikopotentiale zu vermeiden, geht die SySS GmbH wie folgt vor:

- Durchführung des Tests durch ausgebildete und erfahrene Spezialisten.
- Durchführung von Penetrationstests nur nach schriftlichem Auftrag und eindeutiger Testfreigabe für die zu prüfenden Systeme.
- Prüfung der vom Kunden gelieferten Daten auf Korrektheit (z. B. IP-Ranges). Bei Unklarheiten stets Rücksprache.
- Durchführung eines Kick-Off-Workshops anhand eines erprobten Verfahrens inkl. Erstellung eines schriftlichen Protokolls.
- Gute Betreuung im laufenden Projekt.
- Minimierung des Risikos durch Gestaltung des Prüf-Projektes: Langsame Scans (Reduktion der Bandbreite) erhöhen allerdings die Testdauer massiv.
- Tests können auch außerhalb der Geschäftszeit (z. B. nachts/am Wochenende) durchgeführt werden. Wird dieses Vorgehen gewünscht, muss in dieser Zeit ein Ansprechpartner des Kunden direkt zur Verfügung stehen.

- Prüfung von Testsystemen; entspricht das Testsystem aber nur in wenigen Punkten dem produktiven System, muss die SySS GmbH im Bericht stets darauf hinweisen, um seine Aussagekraft nicht zu verfälschen.
- Abbruch des Tests bei erkannten Schwierigkeiten. Indirekt erzeugte Probleme sind für Externe generell nicht erkennbar. Daher muss der Ansprechpartner des Kunden in der Lage sein, Probleme eindeutig dem Test zuzuordnen zu können und vor allem die SySS GmbH zu informieren.
- Wahl von nicht-invasiven Prüfmethode. Die damit einhergehende Reduktion des Erkenntnisgewinns muss dann in Kauf genommen werden. Spekulationen werden als solche im Bericht von der SySS GmbH stets gekennzeichnet.

Die SySS GmbH möchte an dieser Stelle erneut auf die permanente Verfügbarkeit eines Ansprechpartners des Kunden während eines Tests hinweisen, denn ohne diesen kann eine Reihe der oben genannten Punkte unter keinen Umständen erfüllt werden.

Insbesondere sollte der Ansprechpartner auch über die Kompetenz verfügen, mit der SySS GmbH zusammen einen anderen Testverlauf zu planen und gegebenenfalls Schwerpunkte eines Tests zu ändern. Die organisatorischen Prozesse sollten eine gewisse Flexibilität zulassen. Sind beispielsweise die üblichen Ansprechpartner während eines Tests nicht verfügbar, so sind Vertreter zu benennen und mit den entsprechenden Vollmachten auszustatten.

Aufgrund der Erfahrungen der SySS GmbH können die Risiken auf vier technische Ursachen zurückgeführt werden. Diese werden in Kapitel 6.5 gesondert aufgeführt.

## **2.8. Angekündigte oder unangekündigte Prüfungen**

Die Stoßrichtung von Penetrationstests zielt auf die Aufdeckung technischer, keinesfalls menschlicher Defizite ab. Unangekündigte Tests werden aber von den Betroffenen als Letzteres verstanden. Dies hat für den Kunden den großen Nachteil, dass Testergebnisse in Frage gestellt werden und die Motivation der Mitarbeiter, dringende Sicherheitsmaßnahmen umzusetzen, erheblich sinkt. Das Ziel eines Sicherheitstests wird daher in der Regel nicht erreicht, wenn er unangekündigt durchgeführt wird, sondern schlichtweg verfehlt.

Der nachhaltige Erfolg der SySS GmbH besteht darin, dass die Ansprechpartner, Systemverantwortlichen und Administratoren ihrer Kunden der Dienstleistung „Sicherheitstest“ Vertrauen statt Misstrauen entgegenbringen. Ein zentraler Faktor ist hierbei das Angebot an alle Beteiligten, dem Test persönlich beizuwohnen.

**Tipp von Sebastian Schreiber:**

Sprechen Sie mit allen Beteiligten über geplante Tests. Damit erreichen Sie, dass der Sicherheitstest als nützliche Dienstleistung aufgefasst wird und die Ergebnisse effizient bearbeitet werden.

## 2.9. Social Engineering

*Social Engineering*<sup>1</sup> gehört neben allen technischen Möglichkeiten und Gegebenheiten zu den wirksamsten Mitteln, um an sensible Daten zu gelangen. *Social Engineering* bedeutet ursprünglich „angewandte Sozialwissenschaft“, wird aber im Sinne von „sozialer Manipulation“ verstanden und umfasst den professionellen Betrug von Menschen. Die Betrüger geben sich als befugte Techniker oder externe Dienstleister aus und schaffen es, durch ihr angepasstes Auftreten erfolgreich gewünschte Informationen abzufragen. In der Regel haben sie auch hinreichende Kenntnisse der Unternehmenskultur, um hektische Situationen (z. B. IT-Umstellungen in großem Maßstab, Umzüge, hektische und chaotische Situationen aller Art, etc.) dreist ausnützen zu können.

Obwohl *Social Engineering* eine der größten Gefahren für Unternehmen birgt und die Diskussion um Maßnahmen zur Eingrenzung dieses Gefahrenpotentials durchaus berechtigt ist, gibt es einen entscheidenden Unterschied zu allen anderen Testmöglichkeiten: Der Testgegenstand ist hierbei der Mensch und keine technische Komponente. Da ein Mensch aber nicht mit einer indifferenten Maschine gleichzusetzen ist, verfehlen derartige Tests ihr vermeintliches Ziel. Menschen reagieren sehr sensibel auf dieses Thema und sind gegenüber Versuchen in diesem Bereich oft sehr kritisch eingestellt. Sie bewerten solche „Tests“ meist als ethisch fragwürdig und fassen sie ausschließlich als unmenschliche Kontrollmaßnahmen auf, die daher in einem Unternehmen eher zu Schaden führen, anstatt zu einer nachhaltigen Stärkung der inneren Sicherheit.

---

<sup>1</sup> Zu mehr Informationen und zum besseren Verständnis, siehe: [http://de.wikipedia.org/wiki/Social\\_Engineering](http://de.wikipedia.org/wiki/Social_Engineering)

Ferner müssen Prüfer bei solchen Tests eine falsche Identität annehmen und Firmenmitarbeiter unter deren Deckmantel gezielt belügen beziehungsweise in die Irre führen. Außerhalb von scharf kontrollierten Bedingungen ist dies rechtlich kritisch und organisatorisch heikel. Neben einem rechtlichen Schutz für den Prüfer muss auch die Zustimmung des Betriebsrates gewährleistet sein.

Aus den oben erwähnten Gründen empfiehlt die SySS GmbH, *Social Engineering*-Tests nur in Ausnahmefällen in Betracht zu ziehen.

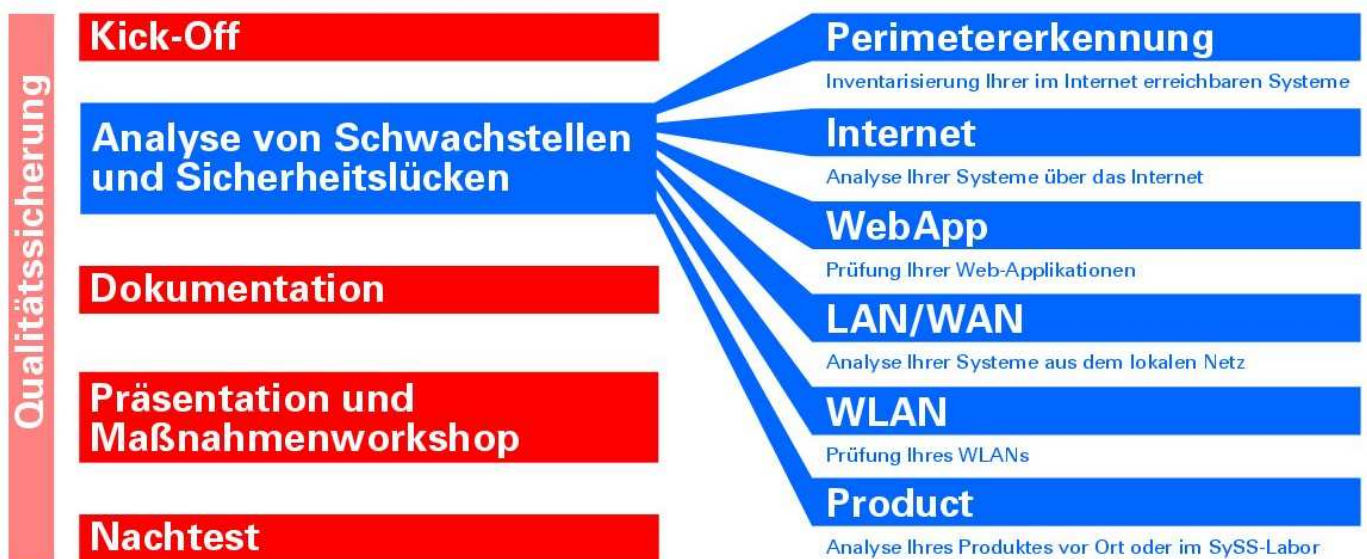
## **2.10. Verdeckte oder offensichtliche Tests**

Bei Sicherheitstests wird – wie bereits erwähnt – nicht verdeckt agiert. Der durchführende Consultant trifft keinerlei besondere Maßnahmen, die Testaktivitäten zu verbergen. Die Erfahrung zeigt, dass Maßnahmen, die zum Beispiel geeignet sind, den Test vor automatisierten Erkennungs- oder Abwehrsystemen (IDS/IPS) zu verbergen, die Testdauer massiv erhöhen – meistens mehr, als einem normalen Projektablauf zuträglich ist.

Anhand des im Rahmen der Dokumentation (Modul DOCU) erstellten Berichtes kann zusätzlich nachvollzogen werden, ob beispielsweise die Tests, die Sicherheitslücken mit hohem Risikopotential nachgewiesen haben, von automatischen Systemen erkannt wurden.

### 3. Projektmodule

Der Sicherheitstest besteht aus einem Rahmenprojekt und einzelnen Testmodulen:



Die Testmodule werden im Folgenden beschrieben. Sollten Ihre Anforderungen durch sie nicht erfüllt werden, sprechen Sie uns an. Dann kann ein individueller Projektplan erstellt werden.

#### 3.1. Kick-Off: KICKOFF

In einer Vorbesprechung (z. B. telefonisch) wird der Projektablauf besprochen. Der Consultant, der den Test leitet, geht daher mit einem Ansprechpartner des Kunden unter anderem folgende Themen durch:

- Testzeitraum und Testzeitfenster
- Ansprechpartner und deren Erreichbarkeit
- Besprechung des Testgegenstandes
- Erfüllungsstand der Voraussetzungen (siehe das jeweilige Modul)
- Umgang mit der Erkennung von DoS-Potentialen
- Allgemeines zur Durchführung (siehe das jeweilige Modul)

- Festlegen der Sprache, in der der Bericht geschrieben werden soll (Englisch oder Deutsch)
- Anzahl der Exemplare des Berichtes, die der Kunde benötigt
- Fragen und Wünsche des Kunden zum Testablauf

Je nach speziellem Testgegenstand und je nach gewählten Modulen gibt es individuelle Abweichungen. Wenn von der Durchführung eines Tests, wie bei den einzelnen Modulen beschrieben, abgewichen werden muss, wird dies ebenfalls zu diesem Zeitpunkt besprochen.

Die Ergebnisse des Kick-Offs werden protokolliert und dem Kunden zeitnah zur Verfügung gestellt.

#### **Tipp von Sebastian Schreiber:**

Prüfen Sie vor dem Kick-Off die unter „Mitwirkung des Kunden“ genannten Punkte und Tipps! Je mehr Zeit Sie sich für die Vorbereitung und die Durchführung des Kick-Off nehmen, desto effizienter wird der Test und desto mehr wird er Ihrem Unternehmen nützen!

## **3.2. Perimetererkennung: PERIM**

### **Zusammenfassung:**

Die SySS GmbH identifiziert Netze und Systeme des Kunden auf der Basis öffentlich verfügbarer Informationen. Der Kunde erhält eine Übersicht über Systeme, die im Internet aktiv sind und zu ihm gehören. Diese kann er für weitere Tests freigeben. Die Perimetererkennung unterstützt interne Inventarisierungsmaßnahmen und die Auswahl zu testender Systeme für weitere Module.

### **Ausgangslage:**

Als Perimeter bezeichnet man die Gesamtheit aller Systeme eines Unternehmens, die vom Internet aus erreichbar sind. Normalerweise werden Sicherheitstests nur auf IP-Adressen durchgeführt, die vom Kunden vorher (auch mit Unterstützung der SySS GmbH) ausgewählt worden sind.

Wenn insbesondere bei großen, international verteilten Netzen des Kunden eine solche Auswahl nicht möglich ist oder wenn die Netze, die getestet werden sollten, erst identifiziert werden müssen, kann eine Perimetererkennung durchgeführt werden.

Ziel ist es, eine Liste von Netzen zu erstellen, die einwandfrei dem Kunden zuzuordnen sind, zusätzliche eventuelle Fehler in der Zuordnung aufzudecken und gegebenenfalls an dieser Stelle Kandidaten für einen Test auszuwählen. Letzteres geschieht nach Verifikation durch den Kunden selbst. Dieser hat hierbei auch die Möglichkeit, Fehler in der eigenen Dokumentation zu korrigieren oder Dienstleister (ISPs) dazu anzuweisen. Aufgrund rechtlicher Rahmenbedingungen kann hier die SySS GmbH nicht selbständig agieren, denn es muss auf jeden Fall ausgeschlossen werden, dass Dritte beeinträchtigt werden.

Gründe hierfür könnten sein:

- nicht dokumentierte Auslagerung von IP-Adressen an Dritte,
- veraltete oder fehlerhafte WHOIS-Einträge,
- gemeinsame Nutzung von Systemen mit Dritten (Bsp. Webhosting)

Der Kunde muss daher zu testende Netze und Systeme freigeben.

Quellen für die Perimetererkennung sind neben frei verfügbaren Datenbanken (WHOIS, DNS) auch das Mail-Routing des Kunden und Inhalte von Webseiten, die eventuell Aufschlüsse über Unternehmensverknüpfungen geben.

#### **Voraussetzungen:**

Um Systeme des Kunden von denen Dritter unterscheiden und Ergebnisse mit seiner Dokumentation abstimmen zu können, sollte auch bei der Perimetererkennung ein Ansprechpartner erreichbar sein.

### **3.3. Analyse aus dem Internet: INTERNET**

#### **Zusammenfassung:**

Systeme im Internet werden auf konkrete Sicherheitsschwächen hin geprüft und die von ihnen ausgehenden Risiken bewertet. Im Rahmen der Dokumentation wird ein Katalog mit Maßnahmenvorschlägen zur Beseitigung der erkannten Sicherheitsschwächen aufgestellt.

### **Ausgangslage:**

Es bestehen zwei Arten von Risiken beim Betrieb von Systemen im Internet. Auf der einen Seite ist es möglich, dass Sicherheitsschwächen in einzelnen Diensten bestehen, die es Dritten ermöglichen können,

- detaillierte Informationen über die Systeme zu gewinnen, die für weitere Angriffe dienlich sind,
- in das System einzudringen und es für eigene Zwecke oder weitere Angriffe zu benutzen,
- Daten zu manipulieren, die nicht von Dritten manipuliert werden sollten.

Auf der anderen Seite besteht die Gefahr, dass unbeabsichtigt Zugriff auf Daten vom Internet aus möglich ist. Dies kann folgende Punkte umfassen:

- Informationen über Systeme und eingesetzte Software können ermittelt werden, die für andere Angriffe nützlich sein können („Information Leaks“),
- Hinweise auf die Namen von Benutzerkonten,
- vertrauliche Daten und Informationen, die nicht system- oder softwarebezogen sind.

Diese Möglichkeit der Informationsermittlung sollte als Risiko nicht unterschätzt werden, da Sicherheitslücken oft nur in Kombination mit genau solchen Hinweisen ausgenutzt werden können.

### **Zielsetzung des Tests:**

Ziel eines Sicherheitstests im Rahmen des Moduls INTERNET ist, die zu testenden Systeme auf die oben genannten Risiken zu prüfen, abhängig von der Testtiefe.

Konkret geht es dabei um die Aufdeckung von Sicherheitslücken bzw. das Finden von Daten, die von einem nicht eingeschränkten Benutzerkreis (Der Internet-Öffentlichkeit) ausgenutzt bzw. ausgelesen werden können.

Wie unter „Aggressivität“ beschrieben, ist das Lahmlegen von Systemen oder Diensten kein Testziel, sondern nur das Aufdecken derartiger Potentiale.

Webapplikationen werden im Rahmen des Moduls INTERNET nicht geprüft, dafür ist das Modul WEBAPP vorgesehen.

Zudem wird im einfachen Vergleich mit anderen getesteten Netzen ein Gesamtüberblick über das festgestellte Sicherheitsniveau erstellt. Eine Werthaltigkeitsanalyse der gefundenen Daten wird nicht durchgeführt, da die Erfahrung zeigt, dass unsere Kunden dies ohne weiteres selbst vornehmen können.

### **Durchführung:**

Die Art der Durchführung wird von dem leitenden Consultant bestimmt, läuft jedoch im Normalfall nach folgendem Schema ab:

- Überprüfung der vom Kunden zur Verfügung gestellten Daten auf Korrektheit
- Identifizierung von Betriebssystemen und erreichbaren Diensten
- Test der erkannten Dienste mit Schwachstellenscannern
- Überprüfung der Ergebnisse, Verifizierung von erkannten Sicherheitslücken
- Einsatz von Werkzeugen, welche Gebiete abdecken, die von Schwachstellenscannern nicht berücksichtigt werden
- Manuelle Prüfungen
- Nachweis von DoS-Potentialen nach Absprache mit dem Kunden

Anhand der vorliegenden Informationen wählt der testende Consultant die Werkzeuge aus, die ihn bei der Erledigung seiner Aufgaben am besten unterstützen. Einige Beispiele finden Sie unter „Werkzeuge“.

### **Mitwirkung des Kunden:**

Damit ein Sicherheitstest effizient und mit hohem Nutzen für den Kunden durchgeführt werden kann, müssen einige Rahmenbedingungen stimmen. Ansonsten wird der Test erschwert oder es treten Verzögerungen (zusätzliche Kosten) ein.

- Die Systeme müssen tatsächlich aus dem Internet erreichbar sein.
- Die Adressen der zu testenden Systeme müssen rechtzeitig vor dem eigentlichen Testbeginn vorliegen.
- Bei der Wahl der Testzeit (im Rahmen des Kick-Off) müssen Wartungsfenster, Zeitonenabhängigkeiten (beim Test von Systemen im Ausland) und Feiertage beachtet werden.
- Ansprechpartner sollten innerhalb der oben genannten Testzeit tatsächlich erreichbar und handlungsfähig sein.
- Die Ansprechpartner sollten einen Überblick über die internen Zuständigkeiten bei den getesteten Systemen haben; dies reduziert den Kommunikationsaufwand während des Tests.
- IDS/IPS-Systeme sollten die testenden Systeme nicht blockieren.
- Die Zuständigkeiten sollten geklärt sein.
- Für den Test von Systemen Dritter muss deren schriftliches Einverständnis vorliegen.

#### **Tipps von Sebastian Schreiber:**

Stellen Sie vor dem Test sicher, dass die betroffenen Mitarbeiter und Systembetreuer informiert sind, damit der Test positiv aufgenommen wird.

Sie können die Testqualität weiter erhöhen, wenn Sie die eigene Dokumentation über die zu testenden Adressen vor dem Test prüfen lassen.

### **3.4. Prüfung von Web-Applikationen: WEBAPP**

#### **Zusammenfassung:**

Ausgewählte Webapplikationen werden aus der Benutzerperspektive auf ihre Sicherheit hin getestet. Es werden Sicherheitslücken gesucht, die auf der eingesetzten Software, ihrer Konfiguration und der Applikationslogik beruhen.

### **Ausgangslage:**

Bei Webapplikationen besteht ein hohes Risiko durch den Verlust an Vertraulichkeit, also dem unautorisierten Zugriff auf Daten. Zusätzlich ist die Kommunikation mit dem Benutzer relevant, denn besonders durch *Cross-Site Scripting (XSS)*-Schwachstellen können sowohl externe als auch interne Benutzer gefährdet werden.

Auch Schwachstellen, die bössartige Änderungen an der Web-Applikation oder deren Elementen ermöglichen, können vorliegen.

Ähnlich wie bei dem Modul INTERNET bestehen auch hier Risiken durch das Eindringen Dritter und die Möglichkeit der (unerwünschten) Informationsermittlung.

Eine Besonderheit bei Webapplikationen sind die meist komplexen Abhängigkeiten von anderen Systemen, zum Beispiel E-Mail und Datenbanken. Diese können durch Schwachstellen in der Applikation ebenfalls beeinträchtigt werden. Im Fall von Datenbanken können selbstverständlich auch Informationen gewonnen werden.

Diese Abhängigkeiten können damit auch von eingesetzter Middleware und im organisatorischen Sinn auch von Lieferanten bestehen.

Zudem wird die Sicherheit einer Web-Applikation nicht allein durch sie selbst, sondern auch durch das verwendete Content-Management-System (CMS) bestimmt.

Eine weitere Besonderheit von Webapplikationen ist, dass Sicherheitsprobleme nach deren Bekanntwerden auch von Laien nachvollzogen werden können; daher besteht die Gefahr von Image- und Vertrauensverlusten.

### **Zielsetzung des Tests:**

Auch hier besteht die Aufgabe darin, festzustellen, ob die oben genannten Risiken vorliegen. Der Bewertung des Risikos einer einzelnen Schwachstelle kommt bei diesem Test eine höhere Bedeutung zu, denn das Vorhandensein eines allgemeinen Problems deutet nicht immer auf ein spezielles Risiko hin.

Des Weiteren ist Testschwerpunkt, ob die Ausnutzung der typischen Schwachstellen von Webapplikationen die Einsichtnahme in Daten anderer Benutzer ermöglicht.

Das Sicherheitsniveau der Anwendung wird abschließend eingeschätzt und Maßnahmen zur Behebung eventueller Schwachstellen vorgeschlagen.

### **Durchführung:**

Die Durchführung ist bei Webapplikationen stark von deren Funktion und Aufbau abhängig. Ein festes Schema für den Testablauf kann daher nicht aufgestellt werden. Der Ablauf entspricht aber grob folgendem Muster:

- Überblickverschaffung von den Funktionen der Anwendungen
- Feststellung möglicher Risiken bzw. Ansatzpunkte für Angriffe, beispielsweise
  - Nutzung fremder/gesperrter Funktionen (z. B. Warenkorb, Benutzerverwaltung)
  - Einsichtnahme in fremde Identitäten
- Zugriff auf gesperrte Daten, Auslesen von Datenbanken
- Manuelle Überprüfung dieser Risiken/Ansatzpunkte
- Suche nach weiteren Ansatzpunkten

Zusätzlich finden bei Bedarf folgende Prüfungen statt:

- Untersuchung des Session-Konzeptes
- Suche nach unerwünscht veröffentlichten Informationen
- Untersuchung der Sicherheit des CMS, falls vorhanden

Schwachstellenscannern, auch solchen, die für den Test von Webapplikationen vorgesehen sind, kommt bei diesem Test eine eher unterstützende Funktion zu, da sie nicht in der Lage sind, kontextbezogene Informationen zu verwerten und zu beurteilen.

### **Mitwirkung des Kunden:**

Für den Test muss auf jeden Fall die URL der Web-Applikation mitgeteilt werden (bezüglich Anmeldedaten siehe unten). Es sollte berücksichtigt werden, dass das verwendete CMS auch mitgetestet wird.

### **Ansprechpartner:**

Die Analyse von Webapplikationen unterscheidet sich nicht nur beim Vorgehen erheblich von anderen Testmodulen. Wie bereits beschrieben, können Sicherheitsprobleme in der Web-Applikation auch weitere Dienste, insbesondere Datenbanken und E-Mail-Dienste, betreffen.

Daneben kommen Webapplikationen bzw. deren Funktionalität in der Regel nicht aus einer Hand: Die Gestaltung kann in den Händen einer Agentur liegen, das Schreiben der Web-Applikation sowohl in den Händen interner als auch externer Programmierer, und die Hardware selbst kann wiederum von einem Webhoster gestellt und auch betreut werden.

Insbesondere zur Behebung der festgestellten Sicherheitsschwächen muss mit denjenigen, die für die betroffenen Elemente zuständig sind, Kontakt aufgenommen werden. Daher ist es von sehr großer Bedeutung, die Kontaktdaten der Ansprechpartner zu kennen, um sie entsprechend kontaktieren zu können.

Wenn es keine direkten Ansprechpartner gibt, kann es zu zweierlei Problemen kommen:

- Rückfragen während des Tests, die zur Verifizierung von Sicherheitsschwächen dienen, können nicht beantwortet werden, was wiederum in Verzögerungen resultiert.
- Wenn die Verantwortlichen für ein Projekt nicht bekannt sind, das von einer Sicherheitslücke betroffen ist, dann verzögert sich die Behebung erheblich.

Aus diesem Grund sollte rechtzeitig vor dem Test mit der Klärung der Zuständigkeiten und Feststellung der Verantwortlichen begonnen werden, auch wenn dies im ersten Schritt aufwendig scheint.

Anschließend sollten die Betroffenen über Termin und Ziel des Tests informiert werden. Ebenso wie bei anderen Testmodulen können sie auf Wunsch dem Test beiwohnen. Falls Dritte betroffen sind, müssen diese der Durchführung des Tests zustimmen (in Form einer Einverständniserklärung).

Zusätzlich sollte während des Tests ein Ansprechpartner, der mit der Web-Applikation aus Benutzerperspektive vertraut ist, für Rückfragen zur Verfügung stehen.

### **Abhängigkeiten:**

Die festgestellten organisatorischen und technischen Abhängigkeiten sollten der SySS GmbH mitgeteilt werden. Dies kann im Rahmen des Kick-Off geschehen.

### **Status der Web-Applikationen:**

Die zu testenden Funktionen müssen möglichst durchgängig verfügbar sein. In einer sehr frühen oder mittleren Umsetzungsphase einer neuen Web-Applikation bringt ein Test keine nachhaltigen Ergebnisse. Er kann aber dennoch sinnvoll sein, wenn möglichst früh entscheidungsrelevante Ergebnisse vorliegen müssen.

### **Anmeldeinformationen:**

Für den Test benötigt die SySS GmbH mindestens zwei Benutzerkonten pro Berechtigungsstufe, aus deren Sicht der Test durchgeführt werden soll. Stehen keine entsprechenden Konten zur Verfügung, kann ein Test nur aus der Perspektive eines Besuchers der Webseite durchgeführt werden. Dies produziert meist keine Informationen über das Sicherheitsniveau der Web-Applikation. Um sinnvolle Ergebnisse zu erhalten, dürfen die Rechte der Benutzerkonten gegenüber denen regulärer Anwender nicht eingeschränkt sein. Über das Verfahren der Erzeugung der Konten wird beim Kick-Off gesprochen.

### **Testdaten/Testsystem:**

Falls der Test nicht an produktiven Daten oder Systemen durchgeführt werden soll, kann auch mit einem Produktivsystem mit Testdaten oder nur mit einem Testsystem gearbeitet werden. Testdatensätze, auf die die für den Test verwendeten Benutzerkonten zugreifen können, sollten bereits vor dem Testbeginn zur Verfügung stehen.

Bei der Arbeit mit reinen Testsystemen ist das Ergebnis des Sicherheitstests nur aussagekräftig, wenn ihre Funktionalität zu großen Teilen mit der des Produktivsystems übereinstimmt.

### **Tipps von Sebastian Schreiber:**

Um bei einem Web-Applikationstest festgestellte Schwächen zu beseitigen, benötigen Sie die Kooperationsbereitschaft des Verantwortlichen für das betroffene Element. Versuchen

Sie, alle Zuständigen und Betroffenen daher frühzeitig festzustellen und zu informieren - nur so ist eine schnelle Reaktion gewährleistet.

Unterrichten Sie alle Beteiligten, auch diejenigen, die beim Test selbst keine aktiven Aufgaben haben. So schaffen Sie zusätzliches Vertrauen in die Dienstleistung Sicherheitstest und stärken die Position der IT-Sicherheit im Unternehmen.

Stehen uns für den Test keine Anmeldeinformationen zur Verfügung, dann ist meist ein nur sehr wenig aussagekräftiger Test möglich.

### **Testwerkzeuge und exemplarische Verwundbarkeiten:**

Die Untersuchung von Webapplikationen kann durch den Einsatz von Security-Scannern bzw. entsprechenden Proxies unterstützt werden. Hier können unter anderem NESSUS, CORE IMPACT, MAXPATROL, SAINT, BURP SUITE PROFESSIONAL und – bei Übernahme der Lizenzkosten durch den Kunden – APPSCAN (WATCHFIRE/IBM) zum Einsatz. Der Einsatz von APPSCAN ist vor allem bei komplexen Applikationen oder beim Test vieler Applikationen innerhalb eines Projektes sinnvoll.

Security-Scannern sind jedoch massive Grenzen gesetzt, daher ist das Hauptwerkzeug bei der Untersuchung von Webapplikationen immer ein Internet-Browser, mit dem manuelle Prüfungen durchgeführt werden. Für FIREFOX (MOZILLA) steht eine große Auswahl an Add-Ons zur Verfügung, daher wird er bevorzugt eingesetzt.

Zusätzlich werden zur tatsächlichen Verifizierung von Schwachstellen Werkzeuge (z. B. Skripte) bei Bedarf erzeugt.

### **URL-Manipulationen:**

Wenn innerhalb einer Webanwendung Parameter an Skripte usw. über die URL übergeben werden, können diese unter Umständen manipuliert werden. Es können dann sowohl unerwünschte Eingaben (z. B. Datenmanipulation von Preisen) vorgenommen als auch Links für *Phishing* konstruiert werden.

## Beispiel:

In einer Webanwendung wird folgende URL verwendet:

```
http://www.shop.com/shoppingcart.asp?Action=Buy&type=special&price=200
```

Der Preis kann editiert werden, um eine URL-Manipulation auszuführen. Werden andere Teile der Webseite über URL-Parameter angesprochen, wie z. B.

```
http://www.shop.com/index.php?session=xd67u9n&url=/specials.html
```

dann können über Änderungen eventuell andere Seiten nachgeladen werden.

```
http://www.shop.com/index.php?session=xd67u9n&url=www.preparedsite.com
```

Ist es möglich, über die Angaben von Pfaden in der URL, Dateien auf dem Webserver einzusehen, so liegt eine *Path- bzw. Directory Traversal*-Verwundbarkeit vor:

```
http://www.shop.com/default.pl?..\..\boot.ini
```

Ist es möglich, über die URL Betriebssystemkommandos auszuführen, dann liegt *Command Injection* vor:

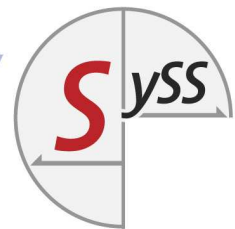
```
http://www.shop.com/default.pl?angebote;uptime
```

Auch an dieser Stelle ist es unter Umständen notwendig, die Eingaben zu kodieren, damit diese ausgeführt werden können.

Die Tragweite von URL-Manipulationen hängt ganz von der jeweiligen Anwendung ab. Daher wird das Risiko durch die SySS GmbH individuell bewertet. URL-Manipulationen verlangen aber als Werkzeug nur einen Browser und keine Spezialkenntnisse, daher besteht stets ein hohes Risiko, dass sie auch ausgenutzt werden.

## XSS-Schwachstellen:

Werden Eingaben in Formularfeldern oder anderen veränderbaren Parametern serverseitig nicht validiert, so kann über diese Code eingeschleust werden, der im Kontext anderer Besucher zur Ausführung gelangt. Diese Angriffsform wird *Cross-Site Scripting* – kurz XSS – genannt, da durch den injizierten Code weitere Code-Fragmente von einem fremden Server nachgeladen werden können. Grundsätzlich wird hierbei zwischen zwei verschiedenen Formen des XSS unterschieden: *Reflected* und *Persistent XSS*.



Bei *Reflected XSS* wird der Angriffsvektor, der den auszuführenden Code enthält, üblicherweise in einem URL-Parameter untergebracht. Dieser Parameter fließt serverseitig in die Generierung einer dynamischen Webseite mit ein und der eingefügte Code kommt beim Aufruf der URL durch einen Besucher in dessen Webbrowser zur Ausführung.

### **Beispiel für *Reflected XSS*:**

Wird die URL einer Webseite aufgerufen, die einen verwundbaren Parameter (hier: „user“) enthält, der serverseitig nicht ausreichend validiert, jedoch in die dynamisch generierte Webseite eingebaut wird, so wird der an diesen Parameter übergebene Code ausgeführt. In diesem Beispiel öffnet sich ein JAVASCRIPT-PopUp-Fenster, welches den Text „XSS“ enthält:

```
http://www.seite.de/login.php?user="><script>alert('XSS')</script>
```

Derartig manipulierte URLs werden häufig in Form betrügerischer E-Mails oder in frei zugänglichen Webforen oder -blogs verbreitet.

Dies ist bei *Persistent XSS*-Schwachstellen nicht nötig, da der Code dauerhaft auf Serverseite gespeichert und bei jedem Aufruf der betroffenen Webseite ausgeführt wird. Das Grundproblem bleibt jedoch das gleiche: von Benutzern änderbare Parameter werden nicht ausreichend gefiltert.

*Persistent XSS*-Schwachstellen sind häufig in Benutzerprofilen oder Kommunikationsfunktionen wie Foren oder kommentierbaren Beiträgen anzutreffen.

### **Beispiel für *Persistent XSS*:**

Eine Webanwendung erlaubt es den Benutzern, Kundendaten zu verwalten. Bei der Eingabe von Kommentaren zu einem Kunden (z. B. „nicht vor 10 Uhr anrufen“) wird diese nicht validiert und Folgendes ist daher als Eingabe möglich:

```
<script>alert('XSS')</script>
```

Ruft nun ein weiterer Benutzer die Daten des Kunden auf, dessen Kommentarfeld entsprechend manipuliert wurde, so erhält er ein Pop-Up-Fenster, das den Text „XSS“ enthält.

Beim Auftreten von XSS-Schwachstellen kann abhängig von der zur Verfügung stehenden Testzeit geprüft werden, inwieweit komplexere Eingaben möglich sind, die zum Beispiel Session-Diebstahl (siehe unten) erlauben. Dies ist nicht immer möglich, daher wird das von XSS-Schwachstellen ausgehende Risiko von der SySS GmbH individuell bewertet.

Unter Umständen können XSS-Schwachstellen von Security-Scannern gefunden werden, die dazu in Formularfeldern vordefinierte Eingaben vornehmen. In vielen Fällen ist dies aber nur durch Anpassungen an den Eingaben möglich, die Security-Scanner nicht leisten können – hier ist Handarbeit vonnöten.

### **SQL-Injection:**

Bei der *Structured Query Language* (SQL) handelt es sich um eine Abfragesprache für relationale Datenbanken. Diese Datenbanken übernehmen in vielen Webapplikationen die Aufgabe der Speicherung von Informationen. Anwender fragen über entsprechende Eingabefelder die Datenbank ab und die Ergebnisse werden von der Anwendung aufbereitet. Erfolgt keine ausreichende Prüfung der Eingaben, so können Anfragen direkt in SQL an die Datenbank gestellt werden; dies wird als *SQL-Injection* bezeichnet.

Innerhalb dieses Kontexts ist zu prüfen, inwieweit darüber Inhalte ausgelesen werden können, die der entsprechende Benutzer anhand seiner Rechte nicht lesen dürfte oder ob Manipulationen an der Datenbank möglich sind.

### **Beispiel:**

Eine Anwendung bietet eine Suchmaske an, über die es unter anderem möglich ist, Benutzer nach ihrem Standort zu suchen. Dabei wird intern folgender Befehl verwendet, um beispielsweise die Abfrage nach dem Standort „London“ zu bearbeiten:

```
SELECT * FROM User WHERE location='London'
```

Da Eingaben nicht überprüft werden, wird folgende Suchabfrage direkt in den Suchbefehl eingebaut:

```
London';DROP TABLE User --
```

Der resultierende Befehl lautet folglich:

```
SELECT * FROM User WHERE location='London';DROP TABLE User --'
```

Das Kommando „DROP TABLE“ löscht nun die Tabelle „User“ aus der Datenbank. Die Kommentar-Zeichenfolge „--“ wird verwendet, um Befehle, die danach getätigt werden, zu ignorieren. Derartige zerstörerische Tests werden bei Sicherheitstest nicht durchgeführt, verdeutlichen aber das enorme Risiko, das von *SQL-Injection*-Schwachstellen ausgehen kann.

SQL-Datenbanken werden auch für die Authentifizierung der Benutzer an der Anwendung selbst verwendet. Werden an dieser Stelle die Eingaben nicht ausreichend geprüft und können daher SQL-Befehle direkt eingegeben werden, kann der Authentifizierungsmechanismus eventuell komplett umgangen werden.

### **Beispiel:**

Folgender Befehl wird intern zur Authentifizierung verwendet:

```
SELECT permission FROM Users WHERE user='$user' AND pass='$pass'
```

Dies führt dazu, dass der folgende Benutzername von der Anwendung akzeptiert (und nicht verworfen) wird:

```
meier' OR '1'='1'
```

Die vollständige, an die Datenbank gestellte Abfrage hat folgende Form:

```
SELECT permission FROM Users WHERE user='meier' OR '1'='1' AND  
pass='$pass'
```

Die ursprüngliche Anfrage verlangt, dass sowohl Benutzername als auch Passwort angegeben werden. Das durch die Manipulation eingefügte logische „OR“ macht diese letzte Bedingung optional. Falls der Benutzername in der Datenbank vorhanden ist, so ist die Authentifizierung erfolgreich.

Derartige *SQL-Injection*-Schwachstellen, die es erlauben, die Benutzerauthentifizierung vollständig zu umgehen, stuft die SySS GmbH als hohes Risiko ein. Sie kompromittieren die Sicherheit einer Anwendung vollständig.

### **Session-Diebstahl:**

Kontrolliert wird, ob es möglich ist, Zugriff zu einer authentifizierten Session eines dritten Benutzers zu erlangen und damit dessen Identität innerhalb der Anwendung zu übernehmen. Gesteuert wird der Zugriff auf eine Anwendung mit einer Session-ID. Diese kann in Form eines Cookies lokal auf der Festplatte des Anwenders gespeichert sein oder bei jedem Aufruf in der URL oder als verstecktes Formularfeld übergeben werden.

### **Beispiel:**

Eine per URL übermittelte Session-ID könnte wie folgt aussehen:

```
http://www.example.net/view/7AD30725122120803
```

Die Session-ID eines Benutzers kann vor allem durch XSS-Angriffe gestohlen werden. Über die XSS-Schwachstelle werden speziell vorbereitete Befehle (z. B. JAVASCRIPT-Code) von einem dritten System geladen und im Browser des Benutzers ausgeführt. Diese lesen seine Session-ID aus und leiten sie weiter. Der betroffene Benutzer muss dabei beispielsweise nur einen modifizierten Eintrag in einem Forum oder eine Beschreibung in einer Produktdatenbank im Webbrowser betrachten. In der Regel ist dem Benutzer nicht bewusst, dass er Opfer eines XSS-Angriffs wird.

Resultat eines erfolgreichen Session-Diebstahls ist daher immer die Übernahme der Identität des betroffenen Benutzers innerhalb der Anwendung. Die SySS GmbH stuft daher einen möglichen Session-Diebstahl immer als hohes Risiko ein.

## **3.5. Sicherheitstest im internen Netz: LAN/WAN**

### **Zusammenfassung:**

Systeme in lokalen Netzen werden auf konkrete Sicherheitsschwächen hin geprüft und die von ihnen ausgehenden Risiken bewertet. Im Rahmen der Dokumentation wird ein Katalog mit Maßnahmen zur Beseitigung der erkannten Sicherheitsschwächen erstellt. Schwerpunkt ist die Feststellung von Sicherheitslücken, die ein hohes Innentäter-Potential haben.

### **Perspektive vor Ort:**

Bei dem Test können zwei Perspektiven eingenommen werden:

Zum einen die Position eines Benutzers mit Zugang zum internen Netz. Systeme werden dann in einem ähnlichen Verfahren wie beim externen Test auf Sicherheitslücken hin untersucht.

Zum anderen kann die Position des Nutzers eines bestimmten Systems („Praktikant“/ „Zeitarbeitskraft“) eingenommen werden. In diesem Fall wird geprüft, inwieweit das System (z. B. der Standard-Desktop für die jeweilige Nutzergruppe) gegen Manipulationen geschützt ist und ob es für Angriffe verwendet werden kann.

Aufgrund der enormen Anzahl an testbaren Diensten, die es typischerweise in internen Netzen gibt, kommt der Auswahl sinnvoller Stichproben eine sehr hohe Bedeutung zu. Dies sollte beim Kick-Off unbedingt besprochen werden.

### **Besonderheiten:**

In internen Netzen können eine Vielzahl von Diensten und Protokollen zum Einsatz kommen. Die Kompetenz der SySS GmbH liegt dabei im Test von IP-basierten Systemen in Ethernet-Netzen.

Bei sehr großen oder sehr komplexen internen Netzen kann die SySS GmbH bei der Auswahl geeigneter Stichproben helfen und gegebenenfalls auch eine Inventarisierung durchführen, die grob der Perimetererkennung entspricht.

### **Ausgangslage:**

Im Gegensatz zu Systemen im Internet, denen ein Risiko von einem nicht einzuschränkenden Benutzerkreis droht, geht es im internen Netz („Corporate Network“) um das Risiko, das von Innentätern ausgeht.

Konkret ist damit ein Benutzer mit Zugang zum internen Netz gemeint. Dieser hat aufgrund seiner Position automatisch einen höheren Kenntnisstand über das ihn umgebende Netz. Dies trifft auch auf Besucher eines Gebäudes zu.

Des Weiteren geht ein Risiko von der versehentlichen Einschleppung von *Malware* (*Malicious Code*) aus. *Malware* kann Sicherheitslücken automatisiert ausnutzen.

Zusätzlich ist das Risiko höher, wenn der PC von Benutzern direkt für Angriffe verwendet werden kann.

### **Zielsetzung des Tests:**

Ziel ist, je nach eingennommener Perspektive (siehe oben) die entsprechenden Risiken aufzudecken, zu bewerten und Vorschläge zur Behebung zu machen. Konkret muss bei nachgewiesenen Sicherheitslücken das Innentäter-Potential eingeschätzt werden. Dabei werden nicht nur reine Sicherheitslücken betrachtet, sondern auch Konfigurationen oder die Verfügbarkeit bestimmter Software, die einem Innentäter Ansatzpunkte für einen erfolgreichen Angriff geben könnten.

Hierbei wird nicht nur die Verwundbarkeit von einzelnen Systemen eingeschätzt, sondern auch die Kommunikation von Diensten untereinander, um *Man-in-the-Middle*-Potentiale festzustellen.

Falls andere Sicherungsmaßnahmen (Update, Ersatz) nicht greifen, wird vorgeschlagen, dass die betroffenen Systeme intern abgeschottet werden.

Die SySS GmbH führt hierbei keine organisatorische Dateizugriffsberechtigungsprüfung durch. Derartige Kontrollen sind oft durch Externe nicht möglich.

### **Durchführung:**

Vom Prinzip ist die Durchführung an die des Moduls INTERNET angelehnt:

- Prüfung der Systeme auf erreichbare Dienste
- Test der Dienste mit automatischen Schwachstellenscannern
- Verifizierung der Ergebnisse
- Begleitende und manuelle Prüfungen
- Bei Bedarf Prüfung der eingesetzten Protokolle auf *Man-in-the-Middle*-Potentiale

Eine Sonderform des Sicherheitstests im internen Netz stellt die Prüfung eines PC-Arbeitsplatzes (beschrieben unter „Perspektive des Tests“) dar. Hierbei wird überprüft, ob direkte Manipulationen an der Hardware möglich sind (Booten von externen Medien) und

anschließend, welche Möglichkeiten das Betriebssystem bzw. die Installation selbst für Manipulationen bietet.

In internen Netzen werden häufig Systeme eingesetzt, die zum einen gegen Angriffe nicht besonders widerstandsfähig sind und zum anderen teilweise weit über ihren Lifecycle hinaus betrieben werden. Das Risiko, dass solche Systeme beim Test abstürzen, ist sehr hoch. Daher ist bei der Prüfung solcher Systeme eine enge Koordination mit dem Ansprechpartner nötig.

Generell empfiehlt die SySS GmbH, Systeme, die das Ende ihres Lifecycles erreicht haben oder seit dem Jahr 2005 nicht mehr gepflegt worden sind, nur zu testen, wenn der direkte Nachweis erbracht werden soll, dass Systeme abzuschotten oder zu ersetzen sind und der entstehende Schaden vom Kunden in Kauf genommen werden kann. Falls möglich, sollten auch für solche Tests Systeme ausgewählt werden, die keine kritischen Funktionen erfüllen. Eine Haftung für alle aus eventuellen Abstürzen oder anderen Beeinträchtigungen entstehenden Schäden wird durch unsere AGB ausgeschlossen.

#### **Mitwirkung des Kunden:**

Für einen internen Test müssen gewisse logistische Voraussetzungen erfüllt werden, vor allem, da er keine autarke Dienstleistung ist.

#### **Ansprechpartner:**

Ein Ansprechpartner sollte während der gesamten Testzeit gut und schnell erreichbar sein. Er kann dem Test gerne beiwohnen. Da der Test vor Ort stattfindet, sollten alle organisatorischen Rahmenbedingungen bereits bei Testbeginn erfüllt sein.

#### **Information der Beteiligten:**

Alle Systemverantwortlichen, Administratoren und anderen betroffenen Mitarbeiter sollten vor Beginn des Projekts über den Test und seine Zielsetzung informiert werden. Ihre Kooperation kann während des Tests nötig sein, ist aber vor allem für die Behebung eventuell gefundener Schwachstellen von essentieller Bedeutung.

### **Arbeitsplatz:**

Für den Consultant sollte ein Arbeitsplatz zur Verfügung stehen. Für den Test eines Netzes ist folgendes erforderlich:

- 2 Netzanschlüsse (Ethernet) an das zu testende Netzwerk
- Stromanschluss für 2 Notebooks und Switch (6fach-Steckdosenleiste)
- Platz für 2 Notebooks, Switch und Unterlagen
- möglichst ruhige Umgebung

Für den Test eines Arbeitsplatzes ist erforderlich:

- Platz und Strom für ein Notebook sowie Internetzugang (Dokumentation und Recherche)

Falls Genehmigungen erforderlich sind, um eigene Hardware an dem Arbeitsplatz betreiben zu können, sollten sie rechtzeitig **vor** Testbeginn eingeholt werden.

### **Zugang zu Gebäuden:**

Der Consultant sollte am Testtag das betroffene Gebäude mit seiner Ausrüstung betreten und den oben beschriebenen Arbeitsplatz erreichen und einrichten können. Eventuell notwendige Genehmigungen sollten daher rechtzeitig beschafft werden.

### **Tipps von Sebastian Schreiber:**

Sie können das Ergebnis eines internen Tests qualitativ aufwerten, wenn Sie der Auswahl der zu testenden Systeme sehr viel Sorgfalt angedeihen lassen.

Bei vielen identischen Systemen ist fast immer der tiefer gehende Test von zwei als Stichproben ausgewählten Systemen sinnvoller als eine grobe Prüfung aller.

Ziel eines Sicherheitstests ist das Aufdecken technischer Defizite. Informieren Sie daher alle Beteiligten vor Testbeginn, sodass der Test als eine positive, die eigene Sicherheit stärkende Maßnahme wahrgenommen wird.

### 3.6. WLAN-Test: WLAN

#### **Zusammenfassung:**

Vor Ort wird das WLAN des Kunden auf Sicherheitsschwächen hin untersucht. Zusätzlich wird die Client-Sicherheit geprüft. Im Rahmen der Dokumentation wird das Sicherheitsniveau des WLANs beschrieben, und es werden Vorschläge zur Behebung von Sicherheitsschwächen gemacht.

Die SySS GmbH prüft dabei WLANs nach dem *IEEE*-Funk-Standard 802.11 auf 2.4 und 5 GHz. Andere Funknetze (basierend auf *OWL*, *OPENAIR*, *UHF*, *S-UHF* usw.) sind nicht Bestandteil eines WLAN-Tests.

#### **Ausgangslage:**

WLAN kann – im Gegensatz zu drahtgebundenen Netzen – jederzeit von Dritten erreicht und empfangen werden. Hieraus resultiert die Gefahr des Missbrauches der WLAN-Infrastruktur. Die Bedrohung besteht einerseits in der unberechtigten Nutzung des WLAN und andererseits in der Ausspähung der übermittelten Daten durch Unbefugte. Dies betrifft dann den Teil des Unternehmensnetzes, welcher per WLAN erreichbar ist.

#### **Zielsetzung des Tests:**

Um die oben genannten Risiken ausschließen zu können, werden sowohl die Zugangspunkte (*Access Points*) als auch die WLAN-Clients (z. B. Notebooks) untersucht. Gegenstand der Untersuchung sind in erster Linie die eingesetzten Verschlüsselungs- und Authentifizierungsverfahren sowie die Client-Konfiguration. Bei dieser wird bei der Untersuchung ein Schwerpunkt auf Resistenz gegen *Man-in-the-Middle*-Angriffe gelegt.

Zusätzlich kann eine Inventarisierung des WLAN erfolgen, wobei seine Konfiguration überprüft wird.

#### **Durchführung:**

Der WLAN-Test findet zwangsläufig vor Ort statt. Das genaue Vorgehen hängt stark von der/den zu testenden Lokation/en und der verwendeten WLAN-Infrastruktur ab. Der Ablauf folgt etwa dem folgenden Muster:

- Verifizierung: Entspricht das Vorgefundene den Erwartungen/Informationen?
- Erkennung von Zugangspunkten (APs)
- Untersuchung der Netze hinsichtlich Authentifizierung und Verschlüsselung
- Angriff gegen festgestellte Authentifizierung und Verschlüsselung
- Untersuchung der WLAN-Clients

Bei der Untersuchung von WLAN-Clients ist ein *DoS* zwangsläufiger Bestandteil. Dieser kann aber auf ausgewählte Systeme (z. B. einen Referenz-Client) beschränkt werden.

Eine Auswahl von möglichen Testwerkzeugen wird unter „Werkzeuge“ vorgestellt.

### **Mitwirkung des Kunden:**

Da WLAN-Tests immer vor Ort stattfinden, sollte wie beim internen Test ein ständiger Ansprechpartner stets zur Verfügung stehen.

### **Informationen:**

Vor Beginn des Tests sollten Informationen über die WLAN-Infrastruktur, insbesondere den eingesetzten *Access Point*-Typ und die Art der Authentifizierung zur Verfügung gestellt werden, am besten im Rahmen des Kick-Off.

Des Weiteren sollten alle Beteiligten, also die Systemverantwortlichen für das WLAN, über den Test und seine Intention informiert werden und während des Tests für Rückfragen erreichbar sein.

### **Ansprechpartner:**

Der Ansprechpartner sollte während des Testzeitraums gut erreichbar sein und dem Consultant auch Zugang zu den zu untersuchenden Gebäuden ermöglichen können. Die Erfahrung zeigt, dass es am effizientesten ist, wenn der Ansprechpartner diese Zugangsberechtigungen selbst hat und zudem erteilen kann.

Falls der Consultant Lokationen ohne Begleitung testen soll, sollte pro zu besuchender Örtlichkeit eine Person zur Verfügung stehen, die den Zugang zu Gebäuden und Geländen

ermöglicht und über den Test bzw. Besuch informiert ist. Optional kann der Consultant mit entsprechenden Unterlagen ausgestattet werden.

### **Zugang zu Gebäuden und zum Gelände:**

Die hierfür erforderlichen Genehmigungen müssen zu Testbeginn vorliegen. Dies betrifft sowohl den Zugang für den Consultant selbst als auch für seine Ausrüstung.

Bei der Wahl des Testzeitraumes sollten vor allem Öffnungs- und allgemeine Arbeitszeiten berücksichtigt werden.

Wenn WLAN-Clients getestet werden, sollten Referenz-Clients zur Verfügung stehen oder Stichproben ausgewählt werden.

Wenn mehrere Örtlichkeiten an einem Tag getestet werden sollen, müssen bei der Wahl des Testzeitraums und der Testdauer auch Faktoren wie Verkehrsfluss usw. in Betracht gezogen werden.

### **Tipps von Sebastian Schreiber:**

Beschaffen Sie die notwendigen Genehmigungen für den Zutritt zu Gebäuden rechtzeitig und informieren Sie die Beteiligten. So werden lange und unproduktive Wartezeiten vermieden.

Das Informieren der Beteiligten hilft, dass sie den Test als eine positive Maßnahme und nicht als eine störende Kontrolle wahrnehmen. Sollten sich unter Ihren Mitarbeitern Personen befinden, die Bedenken haben, so laden Sie diese einfach ein, dem Test ebenso beizuwohnen.

## **3.7. Produkt-/Labortests: PRODUCT**

Dieser Test dient für Untersuchungen, deren Tiefe über die Prüfung der Manipulierbarkeit eines Referenz-(PC-)Arbeitsplatzes im Rahmen des Moduls LAN/WAN hinausgehen soll. Testgegenstand sind sowohl multifunktionale Client- und Serversysteme als auch Systeme für einen speziellen Aufgabenbereich (Automaten, Steuerungs- oder Kiosksysteme, tragbare

Geräte, wie z. B. Handies oder Smartphones, usw.). Die Testperspektive ist die einer Person, die physikalischen Zugang zu dem System hat. Der Testumfang muss im Vorfeld definiert werden. Ein typisches Szenario ist die Bewertung des Risikos welches sich aus einem Diebstahl des Systems oder einem Einbruch an seinem Aufbewahrungsort ergibt. Ein anderes wiederum ist die Bewertung des Risikos, welches von einem Missbrauch durch einen regulären (böswilligen) Nutzer des Systems ausgeht.

### **Durchführung:**

Diese ist völlig von dem zu testenden Produkt abhängig und wird daher im Kick-Off besprochen. Je nach Komplexität und Art des zu testenden Produktes ist eine Zeiteinschätzung sehr schwierig; generell wird daher während des Tests der Schwerpunkt darauf gelegt, hohe Risikopotentiale zu identifizieren.

Aktive Tests werden während eines Produkttests nur an der Teststellung selbst durchgeführt, der Test wird nicht ohne Rücksprache und konkreten Auftrag auf andere Systeme des Kunden ausgeweitet. Sollen abhängige Systeme getestet werden, so ist dies auf Wunsch im Rahmen des passenden Moduls (INTERNET, LAN/WAN, WLAN, WEBAPP) möglich.

Schwerpunkt ist sowohl die Suche nach Sicherheitsproblemen, die ausgenutzt werden können, ohne dabei bleibenden Schaden anzurichten (und die so unentdeckt bleiben) als auch solche (Diebstahlszenario), bei denen auf Kundenwunsch hin ein entstehender Schaden in Kauf genommen werden kann. Das Vorgehen wird im Vorfeld abgesprochen und sollte dem Szenario angepasst werden. Bei einem Diebstahl beispielsweise ist nicht davon auszugehen, dass ein Garantiesiegel respektiert wird.

### **Mitwirkung des Kunden:**

Um einen solchen Test durchzuführen, müssen vor allem logistische Voraussetzungen erfüllt werden. So muss entweder der Transport der Teststellung oder der Zugang zu ihr organisiert werden und wie bei anderen Tests auch ein Ansprechpartner für Rückfragen zur Verfügung stehen (ein Ansprechpartner sollte auch mit der Bedienung der Teststellung selbst vertraut sein).

Wenn es sich bei der Teststellung nicht um ein völlig autonomes System handelt, das getrennt von anderen Systemen getestet werden kann, dann muss während des Kick-Off–

Gespräch definiert werden, welche Tests an abhängigen Systemen durchgeführt werden können, und welche Ansprechpartner wiederum für diese zur Verfügung stehen.

Bei dem Kick-Off sollte das Betriebssystem und die Hardwareplattform mitgeteilt werden. Zudem wird besprochen, ob der Testschwerpunkt auf die Kommunikation des Systems zu legen ist, ob Software oder Hardware nachhaltig manipuliert werden können, usw.

#### **Tipps von Sebastian Schreiber:**

Schätzen Sie den Zeitbedarf für einen Produkttest sehr großzügig ein!

Prüfen Sie, mit welchen Systemen Ihr Produkt kommuniziert. In der Regel ist ein vollständiger Test dieser Systeme sinnvoll, wenn es sich ohnehin um eine organisatorische und technische Einheit handelt. Wählen Sie anschließend das passende Modul für den Test.

### **3.8. Dokumentation: DOCU**

Die Ergebnisse der durchgeführten Tests werden in einem Bericht zusammengefasst. Der Bericht enthält im Einzelnen:

- eine Zusammenfassung der Ergebnisse und die Einschätzung des allgemeinen Sicherheitsniveaus („Executive Summary“)
- eine Liste der festgestellten Schwachstellen mit Risikoeinschätzung und Maßnahmen zur Behebung
- eine nachvollziehbare Darstellung des Nachweises jeder erkannten Schwachstelle
- Auszüge aus den Ausgaben der Testwerkzeuge, wo sinnvoll
- Besonderheiten während des Testablaufes
- falls explizit gewünscht, Kommunikationsnachweis mit dem Kunden.

Der Kunde teilt dabei mit, wie viele Exemplare des Berichts benötigt werden.

Der Bericht wird SySS-intern gedruckt und gebunden. Er wird dem Kunden als Einschreiben mit Rückschein (auch im Ausland) verschickt. Zusätzlich erhält der Kunde den Bericht als PDF-Datei.

Auf Wunsch erhält der Kunde die beim Test entstandenen Rohdaten (Ausgaben der Testwerkzeuge) auf CD/DVD. Allerdings werden diese unbearbeitet zur Verfügung gestellt; so werden z. B. Falsch-Positive aus den Ergebnissen der Schwachstellenscanner nicht entfernt.

Soweit nicht anders vereinbart, werden sonst die Rohdaten drei Monate nach Testende bzw. drei Monate nach einem eventuellen Nachtest gelöscht.

Der Dokumentationsaufwand ist bei internen Tests (Modul LAN/WAN) erheblich höher, da insbesondere das Testvorgehen detaillierter beschrieben werden muss. Die Maßnahmen zur Behebung der Schwachstellen werden zudem mit dem Ansprechpartner während des Dokumentationsprozesses besprochen.

Dies ist ein Beispiel für eine Liste von Sicherheitsschwächen mit Maßnahmenvorschlägen:

### 1.3 Gefundene Schwächen

#	Problem	Empfohlene Maßnahme	Risiko	Referenz
1	webapp.company.de: Methode PasswordChange: Sessiondiebstahl über XSS möglich.	Parameter "orig" validieren und Sonderzeichen entsprechend behandeln.	hoch	3.2.4.2 Seite 22
2	IP 127.0.0.7: Eingesetzte Apache-Version weist vermutlich diverse Sicherheitslücken auf.	Überprüfung der eingesetzten Version, ggf. Update durchführen.	mittel	2.1.5 Seite 13
3	IP 127.0.0.7: OWA vermutlich anfällig für URL-Injection.	Überprüfung des Sachverhaltes, ggf. Update durchführen.	mittel	2.1.5 Seite 13
4	webapp.company.de: DoS-Angriffe bereits durch moderate Belastung möglich.	Stabilisierung der Applikation, Verifizierung der Backend-Kapazitäten.	mittel	3.2 Seite 18
5	webapp.company.de: Methode PasswordChange: Phishing-Angriffe durch URL-Injection möglich.	Für Parameter "orig" nur relative Links erlauben.	mittel	3.2.4.1 Seite 20
6	IPs 127.0.0.{3,4,5}: Umgehung des Loadbalancers und direkter, unverschlüsselter Zugriff auf Webserver möglich.	Direkte Zugriffe auf den Webserver blockieren.	niedrig	2.1.3 Seite 11

### 3.9. Präsentations-Workshop: PRES

Die Ergebnisse des gesamten Tests können in der Form einer Präsentation mit Workshop-Charakter beim Kunden vor Ort dargestellt werden. Bewährt hat sich eine zweiteilige Vorgehensweise:

Begonnen wird mit dem Briefing für die Entscheidungsebene („Management Summary“) mit einer Dauer von etwa 30 Minuten. Hier werden grundlegende Ergebnisse des Tests auf strategischer und organisatorischer Ebene besprochen.

Für diesen Teil steht auf Wunsch auch der Geschäftsführer der SySS GmbH, Sebastian Schreiber, zur Verfügung.

Der zweite Teil ist ein technischer Workshop, der für Systemverantwortliche und Administratoren gedacht ist. An dieser Stelle gibt es die Möglichkeit, tiefgreifendere Fragen zu stellen und mögliche Lösungsansätze zu diskutieren. Dieser Teil wird von dem leitenden Consultant des Tests übernommen.

### 3.10. Nachtest: RETEST

#### **Zusammenfassung:**

Der Nachtest hat die Aufgabe, die Wirksamkeit der Behebungsmaßnahmen von Sicherheitsschwächen zu messen, die in vorangegangenen Tests erkannt worden sind.

#### **Ausgangslage:**

Nach der Identifikation der Sicherheitslücken durch einen Test ist deren Behebung fällig. In der Regel ist hierfür keine besondere Beratungsleistung nötig, dennoch sollten die Ergebnisse dieser Behebungsmaßnahmen verifiziert werden.

Etwa nach 2-4 Wochen, aber spätestens nach einem halben Jahr, sollte daher ein Nachtest durchgeführt werden.

Hierbei wird nicht nach neuen Verwundbarkeiten gesucht, sondern der Status der bereits bekannten Situation untersucht und dokumentiert.

Das Vorgehen wird im Vorfeld kurz besprochen.

Als Dokumentation wird das "Executive Summary" des bereits erzeugten Berichtes angepasst.

**Mitwirkung des Kunden:****Ansprechpartner:**

Soweit möglich, sollten beim Nachttest dieselben Ansprechpartner zur Verfügung stehen wie beim ersten Test.

**Tipps von Sebastian Schreiber:**

Terminieren Sie den Nachttest rechtzeitig, nehmen Sie ihn am besten als festen Termin mit in den Testplan auf!

Wird der Nachttest zeitnah durchgeführt, dient er der Sicherheit durch ein positives Ergebnis am meisten, denn der Erfolg der Behebungsmaßnahmen wird bestätigt.

## 4. Besondere Prüfungen

### 4.1. Test von Systemen Dritter (Dienstleister, Lieferanten u.a.)

Systeme und Netze, die technisch eine Einheit bilden, können aus organisatorischer und rechtlicher Sicht von mehreren Unternehmen gepflegt, betreut und damit auch besessen werden.

Beispielsweise können komplette Systeme von Webhostern gemietet oder eine Spam-Filterung in Form einem von Dritten angebotenen Service verwendet werden. Zudem können Systeme, aber auch ganze Netze, gemeinsam von mehreren Unternehmen oder Organisationen genutzt werden. Die besonderen Zusammenhänge bei Webapplikationen werden im Modul WEBAPP beschrieben.

Zum einen ist es sinnvoll, hier bewusst das Gesamtsystem prüfen zu lassen, also Systeme von Dritten einzubeziehen, zum anderen sind solche Zusammenhänge häufig nicht offensichtlich. Falls derartige Zusammenhänge aufgedeckt werden sollen, kann dies, wie bereits erwähnt, im Rahmen des Moduls PERIM vorgenommen oder im kleineren Umfang während des Kick-Off besprochen werden.

### **Voraussetzung:**

Für die Durchführung eines Tests benötigt die SySS GmbH immer eine schriftliche Einverständniserklärung des jeweiligen Betreibers. Daher müssen diese Betreiber bereits in die Planungsphase mit einbezogen werden. Ein anderes Vorgehen ist aus rechtlichen Gründen nicht möglich.

Um den Test effizient gestalten zu können, sollten auch von Dritten Ansprechpartner für Rückfragen zur Verfügung stehen. Ist die Untersuchung von deren Systemen Hauptbestandteil des Tests, so gelten die Voraussetzungen des jeweiligen Moduls auch für den Dritten.

Im Kick-Off muss geklärt werden, wer über die Ergebnisse des Tests informiert wird, inwieweit der Bericht aufgeteilt werden soll und wie viele Exemplare benötigt werden.

### **Tipps von Sebastian Schreiber:**

Ein hohes Sicherheitsniveau ist die Grundlage für Vertrauen in die Angebote Ihres Dienstleisters. Weisen Sie ihn darauf hin, dass Sie ihm das Angebot machen, das Sicherheitsniveau von der SySS GmbH prüfen zu lassen und auch die Kosten zu übernehmen.

Prüfen Sie bei allen Tests, ob eventuell Dritte betroffen sind. Sorgen Sie rechtzeitig für deren schriftliches Einverständnis. Dritte sollten nicht unvorbereitet mit Testergebnissen konfrontiert werden, da Sie ihre Kooperation für die Behebung von Sicherheitsschwächen benötigen.

Wenn Sie derartige Abläufe vereinfachen möchten, nehmen Sie die Berechtigung zur Durchführung von Sicherheitstests in die *Service Level Agreements* (SLAs) auf.

## **4.2. Forensische Analysen: FORENSIC**

Nach einem beliebigen Sicherheitsvorfall muss dieser näher analysiert werden. Dabei wird untersucht, welche Rückschlüsse auf den Ablauf und unter Umständen sogar auf den Täter gezogen werden können. Die SySS GmbH kann dies durch forensische Analysen unterstützen.

Diese sind in mehreren Varianten durchführbar. Zum einen in der direkten Untersuchung des kompromittierten Systems – der Ablauf entspricht dann grob dem Labortest. Der SySS GmbH wird dabei entweder das System zur Verfügung gestellt oder es wird direkt vor Ort untersucht.

Zum anderen kann Forensik begleitend zu eigenen internen Maßnahmen stattfinden, indem Log-Dateien ausgewertet werden und/oder das betroffene System aktiv auf Sicherheitslücken hin untersucht wird.

### **Mitwirkung des Kunden:**

Selbstverständlich wird für derartige Analysen ein Ansprechpartner benötigt, der Begleitumstände und Hintergründe kennt und auch kurzfristig Kontakt zu den eigentlichen Bedienern vermitteln kann.

Zudem muss geklärt werden, wie die forensische Analyse durchgeführt wird. Ohne extrem präzise Informationen über den Gegenstand der Untersuchung, d.h. technische Details der zu prüfenden Hard- und Software und organisatorische Hintergründe ist der SySS GmbH keine Vorbereitung auf das Projekt möglich. Sollen Projektergebnisse rechtlich verwertet werden, müssen entsprechende Institutionen wie beispielsweise eine Rechtsabteilung frühzeitig informiert werden, damit diese ebenfalls ausreichend Zeit für nötige Recherchen haben.

### **Tipp von Sebastian Schreiber:**

Von allen Tests sind forensische Analysen die individuellsten Projekte, die meine Firma durchführt. Nehmen Sie sich daher genug Zeit für ein ausführliches Vorgespräch!

Bewahren Sie bei ihrem ersten „Fall“ vor allem die Ruhe und gehen Sie das Ereignis sorgfältig mit meinen Mitarbeitern durch. Technische Maßnahmen ohne Klärung der Situation können die forensische Analyse leicht in die falsche Richtung führen und verlängern das Projekt unnötig. Die in die Vorbereitung und Klärung investierte Zeit hat direkten Einfluss auf die Qualität des Ergebnisses der Analyse.

Vermeiden sie vorschnelle Schlüsse (wie z. B. die Nennung von Schuldigen). Forensische Artefakte können in der IT ebenso wie in anderen Fachgebieten mehrdeutig sein. In der

Regel sind sie alleine (z. B. ohne die Informationen, wer ein bestimmtes Gebäude betreten darf oder nicht oder wem ein bestimmtes System zugeordnet ist) von nicht sonderlich hohem Wert.

### 4.3. Prüfung organisatorischer Vorgaben: REVIEW

#### **Ausgangslage:**

IT-Sicherheit kann nur bei Betrachtung als Prozess<sup>2</sup>, nicht durch rein punktuelle Maßnahmen gewährleistet werden. Daher bietet die SySS GmbH Prüfungen der organisatorischen Vorgaben an, welche die IT-Sicherheit definieren. Dies sind Security-Policies, Sicherheits-Handbücher aber auch Regelsets innerhalb der IT-Infrastruktur. Bei Reviews wird das zu prüfende Material unseren Consultants zur Verfügung gestellt, welche sich anschließend damit vertraut machen und sowohl Verbesserungen als auch Änderungen empfehlen. Auf Wunsch können Reviews durch Gespräche oder Workshops abgeschlossen oder flankiert werden. Dieses Modul deckt die nicht-technischen Untersuchungen im Rahmen von Sicherheitstests ab, ist jedoch nicht eigenständig. Um den Status der tatsächlichen Umsetzung von Vorgaben bzw. einer Security-Policy zu kontrollieren, empfehlen wir, zusätzlich das passende Testmodul zu wählen.

#### **Voraussetzungen:**

Die SySS GmbH benötigt zur Durchführung eines Reviews jeweils aktuelle Versionen des zu prüfenden Materials. Ereignisse aller Art können schnell dazu führen, dass die in beliebigen Vorgaben beschriebene Situation mit der realen nicht mehr übereinstimmt - Hinweise darauf sind nur von Mitarbeitern des Kunden erhältlich. Daher ist auch dieses Modul nicht ohne einen Ansprechpartner des Kunden durchführbar, der im Rahmen eines Interviews Rückfragen beantworten oder den Kontakt zu den jeweils Zuständigen vermitteln kann.

---

<sup>2</sup> <http://www.schneier.com/crypto-gram-0005.html>

#### **4.4. Individuelles Anliegen: INDIVIDUAL**

Sollte Ihr Anliegen nicht von den vorgestellten Modulen abgedeckt werden, zögern Sie nicht, uns anzurufen und es uns im Detail darzulegen. Wir werden in fast allen Fällen gemeinsam eine Lösung finden, da wir über langjährige Erfahrung und Expertise in nahezu allen Beratungsbereichen der IT-Security verfügen.

## **5. Grundlagen des Sicherheitstests**

Ein Sicherheitstest wird durchgeführt, um Sicherheitsschwächen verschiedenster Art erkennen und anschließend beseitigen zu können. Im Falle eines Tests durch die SySS GmbH nimmt diese die Erkennung und der Kunde anschließend die Beseitigung vor.

### **5.1. Grenzen von Sicherheitstests**

Ein Sicherheitstest stellt eine Analyse des Ist-Zustandes dar. Risiken, die sich durch mögliche Konfigurationsänderungen oder neue Erkenntnisse in der Zukunft ergeben könnten, lassen sich nur schwer erkennen – derartige Überlegungen haben immer spekulativen Charakter. Um Schlagkraft zu besitzen, müssen Sicherheitstests daher regelmäßig durchgeführt werden.

Zudem sind die Sicherheitslücken, die entdeckt werden können, von der Testperspektive abhängig. Bei einem Test nach dem Modul INTERNET werden zum Beispiel lokale schwache Passwörter nicht entdeckt, wenn es gar keine Möglichkeit gibt, sich an dem zu überprüfenden System vom Internet aus anzumelden.

Ein weiteres Problem ist Budgetknappheit: Werden große Netze oder komplexe Webapplikationen in einem kurzen Zeitraum geprüft, besteht die Gefahr, dass Sicherheitslücken schlichtweg aus Zeitmangel nicht identifiziert werden können. Ein potentieller Angreifer, der sich ausreichend Zeit für eine tiefgehende Untersuchung nimmt, kann diese Sicherheitslücken aufdecken und ausnutzen.

Generell legt ein Sicherheitstest den Schwerpunkt auf die Identifizierung von Schwachstellen, die zum Testzeitpunkt ein hohes, konkretes Risiko darstellen. Daher ist er in diesem Bereich besonders effizient.

## 5.2. Abgrenzung von Sicherheitstests zu anderen Prüfungen

Im Vergleich zu IT-Grundschutz-Audits oder Zertifizierungen nach ISO 27001 ist ein Sicherheitstest vor allem konkreter – er schafft überprüfbare Fakten und benennt direkte Bedrohungen für die IT-Sicherheit.

Sicherheitslücken können auch nachgewiesen werden, wenn BSI-zertifizierte Software eingesetzt wird und ein ISO 27001-Zertifikat vorliegt. Daher sind autonome Sicherheitstests, die von Spezialisten durchgeführt werden, Sicherheitsprüfungen im Rahmen entsprechender Audits vorzuziehen.

Sie stehen dabei aber nicht in Konkurrenz zu derartigen Maßnahmen, sondern eignen sich ideal zur Unterstützung - vor allem, da die Ergebnisse vergleichsweise zügig vorliegen und in ein bestehendes Audit integriert werden können.

## 5.3. Zehn Tipps von Sebastian Schreiber

1. Führen Sie Sicherheitstests auf regelmäßiger Basis durch, z. B. einmal im Jahr.
2. Legen Sie besonderes Augenmerk auf die Prüfung von Web-Applikationen.
3. Definieren Sie die Zeitfenster für Penetrationstests sehr frühzeitig.
4. Sorgen Sie für die tatsächliche Erreichbarkeit und Handlungsfähigkeit des Ansprechpartners Ihres Unternehmens innerhalb dieses Zeitfensters.
5. Die Qualität von Sicherheitstests hängt sehr stark davon ab, wie gut der Informationsaustausch zwischen Dienstleister und Kunden funktioniert. Ihr Ansprechpartner sollte daher frühzeitig benannt und informiert werden.
6. Überzeugen Sie sich von der Arbeitsqualität des Penetrationstesters, indem Sie ihn besuchen und dem Test ein/zwei Tage lang beiwohnen. Laden Sie hierzu gerne auch andere Betroffene (Vorgesetzte, Dienstleister, Kollegen) mit ein.
7. Unangemeldete Tests sind kontraproduktiv, da sie bei Ihren Mitarbeitern eher Misstrauen erzeugen anstatt Vertrauen schaffen.

8. Wählen Sie bei internen Sicherheitstests die zu testenden Systeme sehr sorgfältig aus und seien Sie auf Störungen vorbereitet.
9. Eine organisatorische Vorbereitung des Tests macht sich bezahlt: Nehmen Sie sich Zeit für das Kick-Off.
10. Beauftragen Sie ausschließlich Spezialisten mit Sicherheitstests. Oberflächliche Tests bescheinigen nur vermeintliche Sicherheit.

## 6. Über die SySS GmbH

### 6.1. Firmengeschichte:

Die SySS GmbH wurde 1998 von Diplom-Informatiker Sebastian Schreiber gegründet, um hochwertige Sicherheitstests anzubieten. Gegenwärtig beschäftigt die SySS GmbH achtzehn Mitarbeiterinnen und Mitarbeiter, von denen sich zwölf ausschließlich mit Sicherheitstests beschäftigen.

Kunden der SySS GmbH sind Unternehmen aller Branchen und Größen. Dazu zählen z. B. HEWLETT-PACKARD, ROBERT BOSCH GMBH, KODAK, die EUROPEAN COMMISSION, UNION INVESTMENT, SCHUFA, SAP, INA, T-SYSTEMS, RENAULT-NISSAN-BANK, DEUTSCHE FLUGSICHERUNG, OCE, BUNDESWEHR, DAIMLER AG, MÜNCHENER RÜCK, INNENMINISTERIUM/LKA NIEDERSACHSEN, EUROPÄISCHE ZENTRALBANK, FESTO AG, BURDA SYSTEMS sowie die DEUTSCHE BANK AG. Weitere Referenzkunden finden Sie auf der Homepage der SySS GmbH.

Die SySS GmbH hält Fachvorträge auf nationalen und internationalen Kongressen, bisher in Belgrad, Berlin, Budapest, Bratislava, Bukarest, Dublin, Kiew, Las Vegas, Lissabon, Ljubljana, London, Moskau, München, Paris, Prag, Riga, Wien, Zagreb.

Sie veröffentlicht regelmäßig Artikel in verschiedenen Fachzeitschriften und Printmedien wie SPIEGEL, Stuttgarter Zeitung und Züricher Zeitung. Auch im Fernsehen ist die SySS GmbH präsent, unter anderem im Hessischen Rundfunk, bei WISO im ZDF, im RTL Nachtjournal immer wieder oder bei SternTV.

## 6.2. Besondere Vorgehensweise:

### **Spezialisierung:**

Die SySS GmbH ist auf die Durchführung von Sicherheitstests spezialisiert und bietet zu diesem Thema passende Schulungen an.

Dieser extrem hohe Spezialisierungsgrad sorgt für einen großen Erfahrungsschatz bei allen Consultants, der durch die regelmäßigen Tests ständig weiter ausgebaut wird.

Die SySS GmbH kennt dadurch die Bedürfnisse ihrer Kunden sehr genau und kann ein präzises Testergebnis liefern. Sie bietet den kritischen, aber fairen Blickwinkel des Externen auf das Sicherheitsniveau.

Beratungsleistungen bei der Behebung von erkannten Sicherheitslücken sind dabei nur in minimalem Umfang nötig - um die Umsetzung der nötigen Maßnahmen kümmern sich unsere Kunden sehr erfolgreich selbst.

### **Transparenz:**

Die SySS GmbH legt Wert darauf, dass der Kunde ohne weiteres nachvollziehen kann, wie Sicherheitslücken erkannt und im Rahmen des Tests ausgenutzt worden sind. Denn das Verständnis von Hacking als einem geheimnisvollen, fremdartigen Ablauf schadet der Stärke der Sicherheit im Unternehmen.

Erreicht wird dies durch folgende Punkte:

- Eine hochwertige Dokumentation wird im Rahmen des Moduls DOCU erstellt, deren Ziel die Nachvollziehbarkeit von Sicherheitsproblemen ist.
- Es ist hilfreich, wenn der Kunde seine von Tests betroffenen Mitarbeiter und Dienstleister einlädt, entweder teilweise oder ganz dem Sicherheitstest beizuwohnen. Dabei ist die SySS GmbH jederzeit bereit, dem Kunden mit ihrem Wissen zu dienen.
- Ergebnispräsentation (Modul PRES) durch den Consultant, der den Test geleitet hat.

Nur durch diese Offenheit ist eine positive Wahrnehmung von Sicherheitstests bei den Mitarbeitern möglich.

### **Flexibilität:**

Bei der Durchführung von Tests arbeitet die SySS GmbH nicht nach einem festen Schema, sondern flexibel. Ein festes Schema wäre eine Verkennung der Natur eines Angriffs, denn jedes Netz ist anders und jeder Schritt während des Tests hängt vom vorherigen ab.

Zusätzlich sind sinnvolle Schwerpunktänderungen während des Tests durch ein Gespräch zwischen Ansprechpartner und dem durchführenden Consultant möglich.

### **Qualitätssicherung:**

Die Qualitätssicherung der Berichte, die im Rahmen des Moduls DOCU erstellt worden sind, wird immer von einem weiteren Consultant mit Testerfahrung vorgenommen. Damit wird auch die Nachvollziehbarkeit der Testergebnisse gewährleistet. Falls möglich, kann dies auch bereits während eines Tests geschehen. Zudem sichert das Lektorat der SySS GmbH die sprachliche Qualität des Berichtes.

## **6.3. Werkzeuge:**

Sowohl der genaue Ablauf eines Tests als auch die Auswahl der Werkzeuge liegt in der Verantwortung des testenden Consultants. Dieser passt auf der Basis seiner Erfahrung sowohl den Ablauf an den Testgegenstand und insbesondere an die Testtiefe an und wählt die optimalen Werkzeuge aus. Sowohl die Qualität und Nutzbarkeit als auch die Lizenzbedingungen einer Soft- oder Hardware können sich kurzfristig ändern. Die folgenden Angaben haben beispielhaften Charakter.

Die folgende Übersicht ist daher auch nur eine Auswahl von Werkzeugen, die z. B. bei den Modulen INTERNET und LAN/WAN eingesetzt werden können:

- Für System- und Diensterkennung werden Portscanner wie NMAP, UNICORNSCAN oder WOLPERTINGER eingesetzt.
- Als automatisierte Schwachstellenscanner kommen NESSUS, SAINT und MAXPATROL in Frage.

- Für die weitere Überprüfung einzelner Dienste steht eine sehr große Anzahl von Werkzeugen zur Verfügung wie beispielsweise Relay-Scanner, SMTPMAP/SMTPSCAN, IKE-SCAN, DNSWALK und die HPING-Familie.
- Manuelle Überprüfungen werden von TELNET, NETCAT, SOCAT, CRYPTCAT, OPENSSL und STUNNEL unterstützt.

Für Webapplikationstests setzt die SySS GmbH Proxy-Tools wie die BURP SUITE PROFESSIONAL, den CHARLES PROXY oder WEBCARAB ein.

Zum Test von WLANs setzt die SySS GmbH vor allem AirMAGNET, KISMET, AIRCRACK/AIRCRACK-NG, AIRREPLAY-NG, AIRODUMP sowie KARMA, NETSTUMBLER, HOSTAPD und AIRJACK ein, teilweise mit eigenen Anpassungen.

Die Entscheidung, welche Werkzeuge genau eingesetzt werden, basieren zum einem auf dem zu erwartenden Erkenntnisgewinn und zum anderen auf der Testtiefe. Nicht jedes Werkzeug ist für jede Software einsetztauglich. Der Einsatz eines jeden Werkzeuges hat eine bestimmte Mindestlaufzeit; überschreitet diese den geplanten Testzeitraum jedoch erheblich, muss auf den Einsatz verzichtet werden.

Falls der geplante Testzeitraum es zulässt, können aber auch Werkzeuge zum Einsatz kommen, die beispielsweise erst nach Testbeginn veröffentlicht wurden.

#### 6.4. Grundlegende Ethik für Penetrationstester

Basierend auf schon existierenden Kodizes und über Jahre gesammelten Erfahrungswerten, hat die SySS GmbH den ersten Vorstoß unternommen, eine grundlegende Ethik für Penetrationstester zu erstellen. Diese Ethik wurde in der Ausgabe 04/2009 in der *Datenschutz und Datensicherheit* (DuD) zum ersten Mal veröffentlicht und spiegelt die Einstellung und die Grundlage des Arbeitens bei der SySS GmbH wider. Aufgrund folgender Ethik gestalten wir unsere Arbeit:

- **Unabhängigkeit:** Penetrationstests durchführende Firmen testen nur in solchen Unternehmen, in denen sie weder bei der Konzipierung der IT-Umgebung noch der Einrichtung von Sicherheitsmaßnahmen beteiligt gewesen sind und an die sie auch

keine eigene Software verkauft haben oder verkaufen wollen. Nur so kann sichergestellt werden, dass die Ergebnisse des Tests objektiv sind.

- **Vertraulichkeit:** Sowohl die Identität der beauftragenden Firma als auch jegliche Einblicke in interne Netzwerke, Strukturen sowie in jegliche Daten, ebenso auch die, die dem Penetrationstester zur Verfügung gestellt werden, sind absolut vertraulich zu behandeln.
- **Provisionsverbot:** Die Annahme von Provisionen oder vergleichbaren Vorteilen ist untersagt.
- **Vorsicht:** Der Kunde ist über mögliche Risiken in Kenntnis zu setzen, die bei den Prüfungen erstehen können.
- **Professionalität und Qualitätsmanagement:** Die Arbeit hat professionell zu erfolgen und ist einem Qualitätsmanagement zu unterziehen. Dabei leistet der Penetrationstester seine Arbeit nach bestem handwerklichem Wissen und ethischem Gewissen.
- **Verbindlichkeit:** Vertraglich zugesicherte und in Beratungsgesprächen mündlich getroffene Zusagen sind von den Mitarbeitern der Penetrationstests durchführenden Firma verbindlich einzuhalten.
- **Objektivität, Neutralität und Transparenz:** Schlussfolgerungen müssen objektiv sein und sind nachvollziehbar darzustellen.
- **Interessenskonflikte:** Interessenskonflikte zwischen Penetrationstestern und Kunden sind zu vermeiden und gegebenenfalls anzuzeigen und auszuräumen.
- **Striktes Legalitätsprinzip:** Die Gesetze der von Penetrationstests betroffenen Länder sind strikt einzuhalten, auch wenn Teilergebnisse eines Penetrationstests selbst einen Interessenskonflikt mit der vorgefundenen Gesetzgebung darstellen könnten. So kann die Aufdeckung von Schwachstellen in bestimmten Fällen Verstöße gegen bestehendes Recht begünstigen. Penetrationstester sind daher verpflichtet, sich mit der jeweiligen Gesetzeslage vertraut zu machen und sorgfältig darauf zu achten, dass ihre Arbeit innerhalb der vorgegebenen Gesetzesgrenzen abläuft.
- **Respekt vor Menschen:** *Social Engineering*-Attacken sind Angriffe gegen das Verhalten von Menschen – diese werden, sofern sie überhaupt realisiert werden, ausschließlich angekündigt durchgeführt.
- **Korrektes Zitieren:** Wird fremdes Wissen bei der Arbeit herangezogen und verwertet, so sind die Quellen/Urheber korrekt auszuweisen.

## 6.5. Beschreibung der technischen Risiken bei Tests

### **Last bei Web-Applikationstest**

Bei Sicherheitstests wird, ähnlich wie bei Funktionstests, Last auf der Datenbank erzeugt, die die Web-Applikation versorgt. Dies kann beispielsweise eine Suche über alle Felder sein, die dem Nutzer der Anwendung scheinbar nicht möglich ist. Ist das System, auf welchem die Datenbank läuft, sehr knapp kalkuliert oder schlichtweg in die Jahre gekommen, kann dies zu Beeinträchtigungen führen. An dieser Stelle ist eine manuelle Betreuung der Datenbank durch Mitarbeiter des Kunden nötig - denn von externer Seite aus kann nur die Frequenz der Suchanfragen verändert werden; die Priorität einer Suche gegenüber anderen nicht.

### **E-Mails an interne Adressen**

Über entsprechende Funktionen können über die Web-Applikation E-Mails verschickt werden, zum Beispiel Produktanfragen. Diese dürfen sich weder für Spam-Versand noch für das Fälschen von E-Mails missbrauchen lassen. Probleme ergeben sich an dieser Stelle fast ausnahmslos durch am Mailversand beteiligte Systeme, die eine Serie automatisch erzeugter Nachrichten nicht schnell genug abarbeiten können. Auch an dieser Stelle ist eine manuelle Betreuung der beteiligten Systeme nötig, da von externer Seite aus über die Komposition der beteiligten Systeme nur Annahmen gemacht werden können.

Die SySS GmbH empfiehlt an dieser Stelle, derartige Systeme nicht auf ein sehr niedrig geschätztes Nutzungsvolumen auszulegen, sondern hinreichende Leistungsreserven vorzusehen. Diese können auch durch Optimierungen an der Datenbank und den Suchroutinen in der Web-Applikation gewonnen werden.

Allerdings sind bei der Verwendung von Alt- oder Uraltssystemen der Lastreduzierung durch Optimierung an der Datenbank klare Grenzen gesetzt.

### **Ausfall von Infrastrukturkomponenten**

Sicherheitstests erzeugen einen gewissen Netzwerkverkehr, den die beteiligten Komponenten, Router und Switches abwickeln müssen. Von ihnen wird dabei dasselbe korrekte Funktionieren wie im regulären Betrieb erwartet. Die bei einem Sicherheitstest

entstehende Last entspricht in ihrer Natur auch der Last, wie sie eine intensive Nutzung zahlreicher Kommunikationsdienste hervorrufen würde. Infrastrukturkomponenten, die bei solchen Tests ausfallen statt einfach langsamer zu werden, sind extrem kritisch zu betrachten. Auch wenn sie höher liegt als bei legitimer Nutzung, so ist die Last eines Sicherheitstests nicht einmal ansatzweise mit der eines verteilten Angriffes (*DDOS*) zu vergleichen. Zudem besteht das Risiko, dass die Systeme auch natürlich auftretende Lastspitzen nicht abfangen können. Dies kann z. B. die positive Annahme eines neuen Angebotes durch den eigenen Kundenstamm sein oder Reaktionen der Öffentlichkeit auf Nachrichten.

In der Regel lassen sich derartige Vorfälle eindeutig auf die eingesetzte Hardware bzw. die auf ihnen laufende Software zurückzuführen. Wird diese ohnehin vom Hersteller nicht mehr unterstützt, so empfiehlt die SySS GmbH ein Upgrade. Reduziert werden kann das Risiko durch ein langsames Vorgehen beim Testen, welches aber die für das Projekt nötige Zeit leicht vervielfachen kann.

### **Nicht ausreichende Leitungskapazität**

Die SySS GmbH verwendet für Tests hauptsächlich Root-Server im Internet. Sowohl die Systeme als auch die eingesetzten Werkzeuge selbst sind für jedermann verfügbar. Die bei einem Sicherheitstest nötige Last kann daher von Dritten mit vergleichsweise geringem finanziellem Aufwand ebenfalls erzeugt werden. Dies bedeutet konkret, dass jeder Breitbandanschluss in der Lage ist, eine 2 M/Bit-Strecke zu überlasten oder zumindest massiv zu beeinträchtigen.

Bestimmend für das Risiko ist neben der Leitungskapazität ausschließlich der Faktor Zeit. Eine Reduktion der benötigten Bandbreite wird immer mit einer längeren Dauer des Tests verkauft. Alternativ sind nur Stichproben möglich.

Da die Leitungskapazität von externer Seite nur indirekt und unpräzise festgestellt werden kann, ist die SySS GmbH daher auf präzise und nicht-widersprüchliche Informationen ihres Kunden angewiesen. Die SySS GmbH hat an dieser Stelle keine Einsicht in die Verträge oder Absprachen des Kunden mit seinen Providern und kann daher diese Informationen nicht selbst erbringen.

Generell empfiehlt die SySS GmbH, die Leitungskapazität modernen Erfordernissen anzupassen. Werden beispielsweise mehrere Class-C-Netze von einer 2 M/Bit-Strecke versorgt, so gibt es in der Regel bereits Beeinträchtigungen durch die nicht ausreichende Bandbreite.

Auf der anderen Seite können Kosten reduziert werden, indem einzelne Systeme im Ganzen oder teilweise extern gehostet werden.

Ist dies nicht möglich, weil zum Beispiel Leitungen mit entsprechender Kapazität vor Ort nicht für einen vernünftigen Preis zu haben sind, empfiehlt die SySS GmbH, ein klares Konzept für den Fall aufzustellen, dass die Leitung versehentlich – keinen bösen Willen vorausgesetzt – überlastet wird und die alltägliche Nutzung dann nicht mehr möglich ist. Der Ansprechpartner des Kunden sollte in diesem Fall der jeweilige Provider sein.

## 6.6. Veröffentlichungen der SySS GmbH (Auswahl)

Die SySS GmbH veröffentlicht regelmäßig Artikel in Fachzeitschriften oder auf Kongressen. Hier eine Auswahl:

Deeg, Matthias: *SySS knackt weiteren USB-Stick*, SySS Publikation, [www.syss.de](http://www.syss.de) , 02/2011

Deeg, Matthias: *Rechteausweitung mittels Antivirensoftware*, SySS Publikation, [www.syss.de](http://www.syss.de) , 01/2011

Borrmann, Micha: *Kurze Sicherheitsanalyse von OWOK light*, SySS Publikation, [www.syss.de](http://www.syss.de) , 01/2011

Bott, Christoph/Schreiber, Sebastian: *Bedroht „Hole 196“ die WLAN-Security?* in: VAF Report, Ausgabe 03/2010

Deeg, Matthias/Eichelmann, Christian: *Angriff auf Online-Banking-Applikation*, SySS Publikation, [www.syss.de](http://www.syss.de), 03/2010

Eichelmann, Christian: *SySS späht Daten auf iPhones aus*, SySS Publikation, [www.syss.de](http://www.syss.de) , 02/2010

Schreiber, Sebastian: *Rechtliche Aspekte von Penetrationstests* in: Wirtschaftsinformatik und Management (WuM), 01/2010

Schreiber, Sebastian: *Totgesagte leben länger* in: KES 4/2009

Schreiber, Sebastian: *Vorschlag zum Entwurf einer Berufsethik für Penetrationstester* in DuD (Datenschutz und Datensicherheit) 04/2009

Muncan, Michael/Schreiber, Sebastian: *Interne Penetrationstests – Sicherheitstests im Firmennetz* in DuD 04/2009

Arbeiter, Stefan/Deeg, Matthias: *Bunte Rechenknechte* in: C't 6/2009

Borrmann, Bachfeld: *Zechpreller: Unsichere Bezahlungssysteme* in C't 6/2008

Heinrich, Katrin/Schreiber, Sebastian: *Penetrationstests als Instrument der Qualitätssicherung* in IT Sicherheit und Datenschutz 6/2007

Bott, Christoph/Schreiber, Sebastian: *Penetrationstests – Hackerangriffe als Kontrollinstrument* in: S&I April 2007

Borrmann, Micha/Schreiber, Sebastian: *Sicherheit von Web-Applikationen aus Sicht eines Angreifers* in: DuD -Datenschutz und Datensicherheit, 11/2006

Schreiber, Sebastian: *Suchmaschinen als Hackerwerkzeug* in: PC-Magazin 7/2006

Schreiber, Sebastian: *Securitykosten am Beispiel von Penetrationstests* in: Praxis der Wirtschaftsinformatik, April 2006

Schreiber, Sebastian: *Google Hacks – penetrante Suchmaschinen* in: KES 4/2005

Schreiber, Sebastian: *Hackertools und Penetrationstests* in: HMD 236 - Praxis der Wirtschaftsinformatik, Ausgabe v. 23.4.2004

Kroma, Pierre/Schreiber, Sebastian: *Störfunk - D.o.S. gegen WLANs* in: Heise Security, Ausgabe v. 12.03.2004

Borrmann, Micha/Schreiber, Sebastian: *Wer zählt, gewinnt* in: C't 23/2003, S. 212

Borrmann, Micha: *Unentdeckt Ports scannen* in: Network Computing 10-11/2003, S.46

Schreiber, Sebastian: *Ans Licht gebracht* in: Kommune21 6/2003, S.34f.

Bei Interesse senden wir Ihnen gerne unsere Pressemappe zu, die Artikel von und über die SySS GmbH enthält.