184 Netzwerksicherheit implementieren

Quelle: www.computerweekly.com

Modulunterlagen

Inhaltsverzeichnis

1 Handlungsziele und Handlungsnotwendige Kenntnisse 4
2 Einführung 6
2.1 Über dieses Dokument 6
2.2 Über die Methodik 6
2.3 Dokumentation der Umsetzungen 6
3 Voraussetzungen für Netzwerksicherheit 7
3.1 Netzwerk-Dokumentation 7
3.2 Beurteilung von Netzwerk-Komponenten 11
3.2.1 Aufgabe: Beurteilung von Netzwerk-Komponenten 12
4 WLAN 13
5 Grundlagen von Remote Access-Techniken 14
5.1 Kurzübersicht der VPN-Verfahren 14
5.2 Authorisierungsmethoden 14
5.3 Verbindungsarten 15
5.4 Aufgaben 15
5.4.1 Aufgabe: Next-Generation Firewall-Appliance einrichten 15
5.4.2 Aufgabe: Fernwartung für Firewall absichern 16
5.4.3 Aufgabe: End-to-Site VPN einrichten 17
5.4.4 Aufgabe: Site-to-Site VPN einrichten 17
6 Sicherheit für den WAN-Zugriff 18
6.1.1 Aufgabe: Virtual Appliance einrichten 18
6.1.2 Aufgabe: Web-Filterung einsetzen 19
7 Datenverkehr analysieren 20
8 Intrusion Prevention / Detection System 21
8.1.1 Aufgabe: Umsetzung IPS auf Sophos 21
8.1.2 Aufgabe: Umsetzung IPS als eigenständiger Service 21
9 Beurteilung von aktuellen Exploits 22
10 Überwachen 23
10.1 Aufgaben 23
10.1.1 syslog-ng aktivieren und konfigurieren 23
10.1.2 SNMP einrichten 23
11 Weitere Virtual Appliances kennen lernen 24

Identifikation und Änderungsgeschichte

Dokumenttitel:	184 Netzwerksicherheit implementieren
Thema:	184 Netzwerksicherheit implementieren
Autor:	Dominik Uehlinger, Patrick Kramer
Firma:	RAU, Regionales Ausbildungszentrum Au
Dateiname:	HandOut-184_NetzwerksicherheitImplementieren_v14.docx
Ablageort:	K:\Module_Reform2014\184_NetzwerksicherheitImplementieren\Lernende\HandOut-184_NetzwerksicherheitImplementieren_v14.docx

Version	Datum	Bemerkungen
1.0	Dezember 2016	Initialversion / DU
1.1	Juni / Dezember 2017	Erweiterung von Themen / Aufgaben / DU
1.2	September 2018	Anpassungen / DU
1.3	September 2019	Erweiterungen / DU
1.4	Juli 2020	Anpassungen an Sophos SFOS
1.5	Juni 2022	Anpassungen / PK

1 Handlungsziele und Handlungsnotwendige Kenntnisse

Quelle: ICT-Berufsbildung Schweiz

Modulnummer	184
Titel	Netzwerksicherheit implementieren
Kompetenz	Implementiert, testet und überwacht den sicheren Netzbetrieb sowie den Netzzugang.
Handlungsziele	1. Untersucht ein bestehendes Netz auf Sicherheitslücken und Konfigurationsmängel mit Hilfe der Netzdokumentation und geeigneten technischen Mitteln.
	2. Erarbeitet ein Konzept für den sicheren WAN, WLAN, LAN und geeigneten Remote Zugriff.
	3. Konfiguriert und dokumentiert die Sicherheitssysteme (z.B. Remote Access, Firewall, Proxy, WLAN) gemäss erarbeitetem Konzept.
	4. NIDS nach Vorgaben installieren, konfigurieren und ins Netzwerk integrieren.
	5. Überwacht Netzkomponenten und analysiert Log Einträge der Netzkomponenten.
	6. Implementierte Netzwerksicherheit überwachen.
Kompetenzfeld	Network Management
Objekt	Kommunikationsnetz in einem KMU mit Internet Zugang.

Handlungsziel	Handlungsnotwendige Kenntnisse
1.	1. Kennt die grundlegenden Elemente einer Netzwerkdokumentation. 2. Kennt verschiedene Netzwerkkomponenten und deren Sicherheitseinstellungen. 3. Kennt Tools zum Entdecken und Bewerten von Sicherheitsrisiken. 4. Kennt technische Hilfsmittel zur Analyse (z.B. Portscanner, Sniffer) des Datenverkehrs im Netzwerk. 5. Kennt aktuelle Exploits und deren Angriffswege auf das System.
2.	1. Kennt technische Verfahren für einen sicheren Remote Access (z.B. Protokolle, Standards, Technologien) 2. Kennt aktuelle WLAN Standards und deren Sicherheitseinstellungen. 3. Kennt Konzepte und Sicherheitssysteme und deren Konfigurationsmöglichkeiten (z.B. Härten, DMZ, Remote Access, Firewall, Proxy).
3.	1. Kennt Standardverfahren für die Härtung von Netzwerkkomponenten (z.B. Router, Firewall, Proxy). 2. Kennt gängige Darstellungsarten und Symbole für Netzwerkplan und Netzwerkschema.
4.	1. Kennt die technischen Möglichkeiten und die Funktionsweise eines NIDS.
5.	1. Kennt Verfahren aus den Logfiles sicherheitsrelevante Informationen zu erkennen. 2. Kennt Monitoring-Tools und Protokolle (z.B. SNMP) zur Überwachung der Netzkomponenten.
6.	1. Kennt Möglichkeiten die Informationen des NIDS im operativen Betrieb zu nutzen.

2 Einführung

2.1 Über dieses Dokument

Beim vorliegenden Dokument handelt es sich um ein Aufgabenskript mit Fragen und Querverweisen auf weiterführende Quellen. Daneben sind Wissensteile enthalten, welche für das grundsätzliche Verständnis der Thematik notwendig sind.

Es bestehen für die einzusetzenden Produkte und Technologien umfangreiche Dokumentationen, die sich in hohem Mass als Referenz eignen, gut verständlich und mit Beispielumsetzungen erklärt werden.

Diese Referenzen sowie vertiefte Beschreibungen und Theorien werden über OneNote abgehandelt.

	**SEITE**	Referenz auf die OneNote-Seite unter den «Vorgaben».

2.2 Über die Methodik

Tipp

Pro Themenbereich gibt es neben einer Einführung immer mehrere Aufgaben, welche schrittweise aufgebaut sind. Vor einer praktischen Übungseinheit wird diese jeweils erklärt und teilweise auch demonstriert.

Diese Arbeitsweise zieht sich durch das ganze Modul. Die Erklärungen und Theorieblöcke sind kurzgehalten.

2.3 Dokumentation der Umsetzungen

Sie werden innerhalb von diesem Modul einige praktische Umsetzungen in Gruppen- und Einzelarbeit durchführen. Um dieses praktische Wissen für die Praxis festhalten zu können, ist es ratsam, dieses in einer geeigneten Form zu dokumentieren.

Diese Dokumentation ist ausschliesslich für Ihren Nutzen gedacht. Führen Sie die Dokumentation bereits ab der ersten praktischen Übung und halten Sie sie parallel zur Aufgabe immer auf dem aktuellen Stand.

3 Voraussetzungen für Netzwerksicherheit

3.1 Netzwerk-Dokumentation

Um die Grundvoraussetzungen für ein sicheres und stabiles Netzwerk zu erhalten, ist es unabkömmlich, dass man über die eigene Systemlandschaft Bescheid weiss und einen detaillierten Überblick darüber hat.

Bei einer zweckmässigen Netzwerk-Dokumentation, welche ihrem Namen tatsächlich gerecht wird, ist die Vollständigkeit sowie die Nachvollziehbarkeit der Konfigurationen und Einstellungen das Hauptaugenmerk. Das Ziel ist, dass man anhand dieser Dokumentation alle relevanten Informationen über die gesamte Netzwerk-Umgebung hat und ein aussenstehender Fachmann sich damit zurechtfinden würde.

Der Dokumentations-Inhalt über die Komponenten ähnelt sehr dem des Inventars. Zusätzlich werden auch die Software- oder Firmware-Versionen beschrieben – resp. ein Verweis auf eine vorhandene CMDB (Configuration Management Database) gemacht.

Daneben werden alle Server-Dienste aufgelistet inklusive derer Konfiguration (falls abweichend von der Standard-Konfiguration).

Als Beispiel für eine Dienst-Beschreibung dienen folgende Abbildungen:

10 BACKUP

10.1 Summary

Jede Woche wird ein Backup der gesamten internen Notebook-Festplatte auf die externe Festplatte gemacht.

10.2 Backup Software

Zur Sicherung der Daten wird das in Windows 7 integrierte Programm „Sichern und Wiederherstellen“ genutzt.

10.3 Sicherungsumfang

Es wird jeden Freitag eine Sicherung durchgeführt.

Zeit	Inhalt
Freitag, 12.15 Uhr	Gesamte Festplatte

Abbildung 1: Beispiel Doku 1

2 DNS

Für das Peer-to-Peer Netzwerk ist keine gesonderte DNS-Konfiguration erforderlich. Die DNS-Funktionalität übernimmt der Swisscom-Router. Alle Anfragen an nicht interne Adressen, werden an folgende öffentliche DNS-Server weitergeleitet:

	DNS Server	IP
1.	dns1.bluewin.ch	195.186.1.162
2.	dns2.bluewin.ch	195.186.4.162

3 DHCP

3.1 DHCP Bereiche

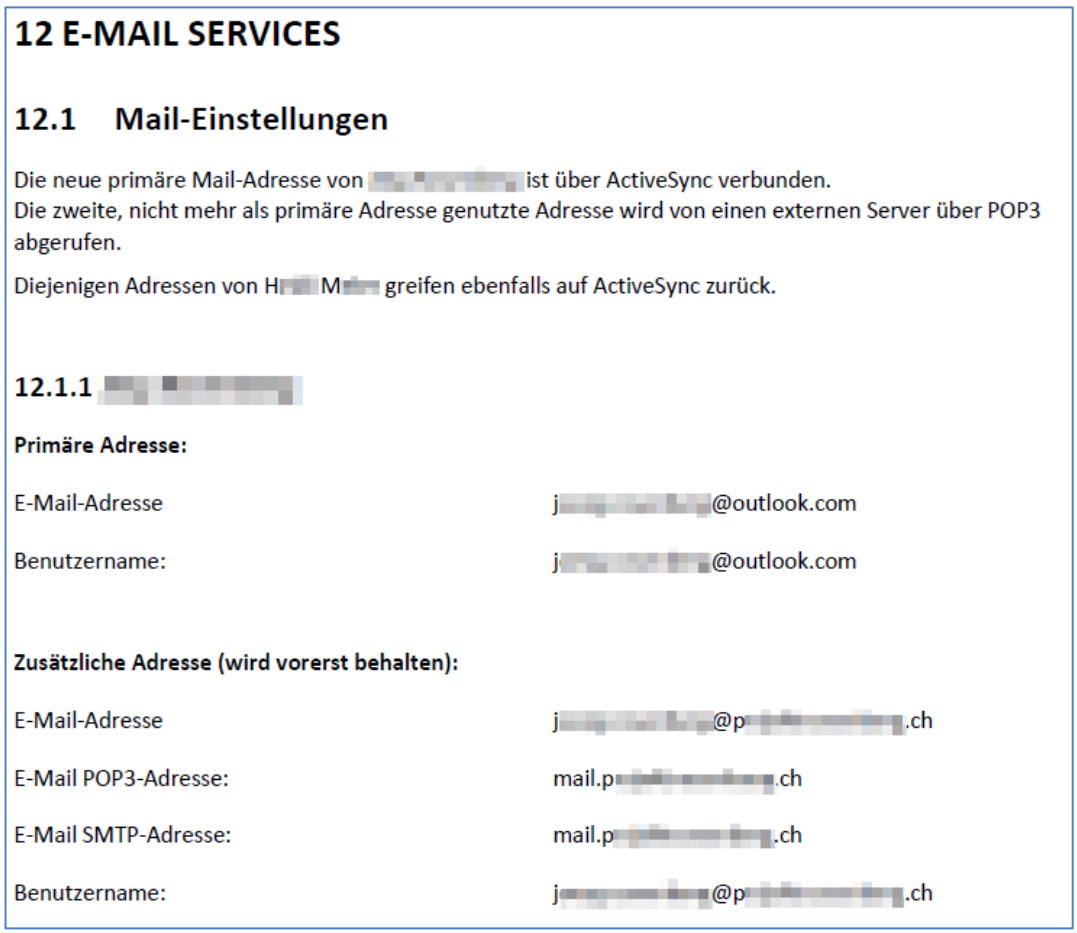
Auf dem Router als DHCP-Server sind die Adressen des Netzwerkes in folgende Bereiche eingeteilt:

Bereich	Typ
192.168.1.115 – 192.168.1.145	Adress-Pool

3.2 DHCP Leasezeit

Leasezeit für eine DHCP Adresse	8 Tage

Abbildung 2: Beispiel Doku 2



12 E-MAIL SERVICES

12.1 Mail-Einstellungen

Die neue primäre Mail-Adresse von [redacted] ist über ActiveSync verbunden.
Die zweite, nicht mehr als primäre Adresse genutzte Adresse wird von einen externen Server über POP3 abgerufen.

Diejenigen Adressen von H[redacted] M[redacted] greifen ebenfalls auf ActiveSync zurück.

12.1.1 [redacted]

Primäre Adresse:

E-Mail-Adresse	j[redacted]@outlook.com
Benutzername:	j[redacted]@outlook.com

Zusätzliche Adresse (wird vorerst behalten):

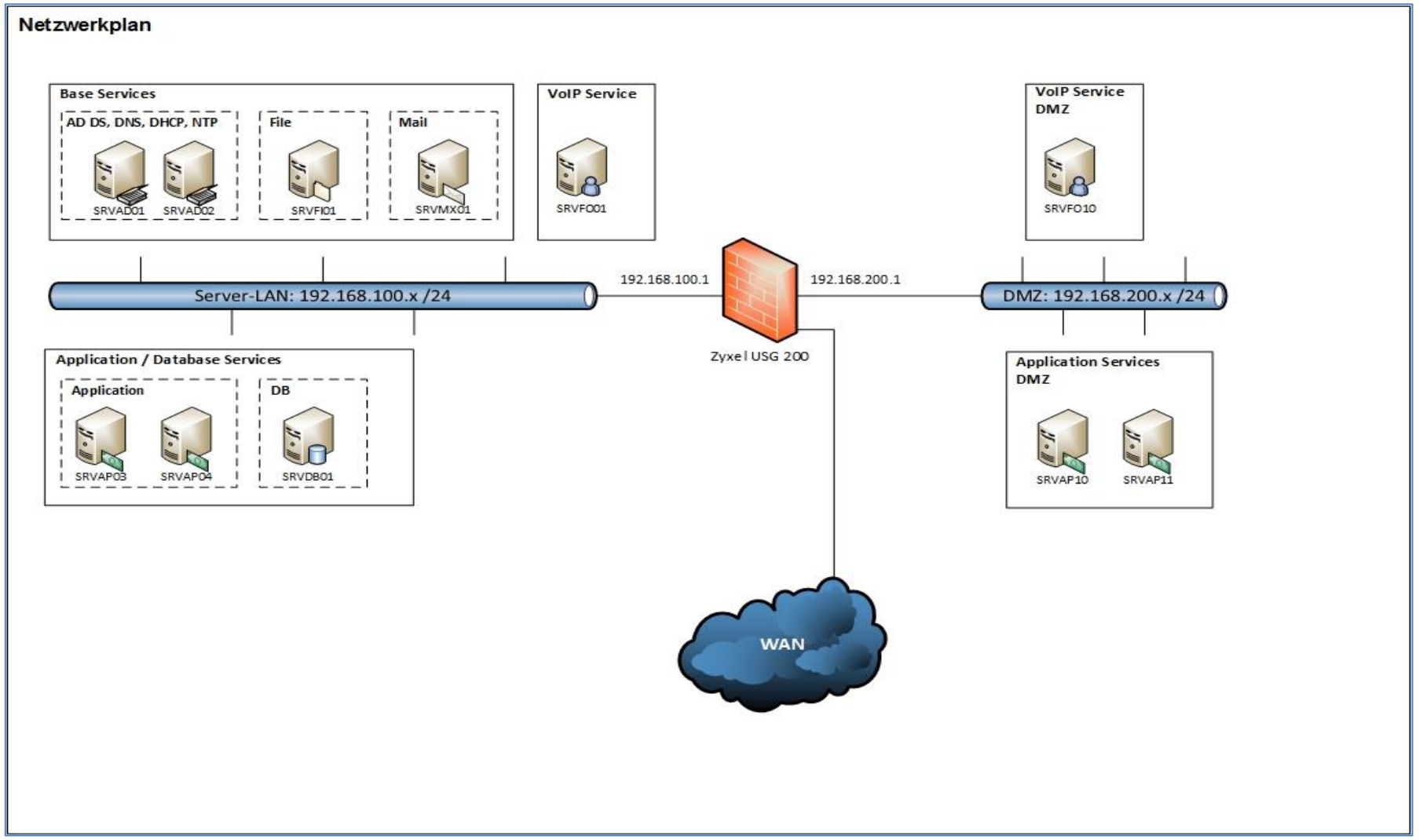
E-Mail-Adresse	j[redacted]@p[redacted].ch
E-Mail POP3-Adresse:	mail.p[redacted].ch
E-Mail SMTP-Adresse:	mail.p[redacted].ch
Benutzername:	j[redacted]@p[redacted].ch

Abbildung 3: Beispiel Doku 3

WICHTIG!

Jegliche Kennwörter gehören nicht in eine Netzwerk-Dokumentation, sondern sollen in einem gesonderten Passwort-Verwaltungs-Tool hinterlegt und gepflegt werden (bspw. KeePass, Password Safe).

Netzwerkplan:



Aufgabe: Netzwerk-Dokumentation

A1	Anhand der vorliegenden Informationen und Hinweise: Wie beurteilen Sie die Netzwerk-Dokumentationen, welche in Ihrem Betrieb eingesetzt werden? Was ist positiv, was ist negativ? Besprechen Sie das in Teams zusammen und halten die wichtigsten Punkte für eine offene Diskussion fest.

3.2 Beurteilung von Netzwerk-Komponenten

Um ein Netzwerk auf Sicherheit zu bewerten, spielen die eingesetzten Netzwerk-Komponenten eine grundlegende Rolle. Sie sind der Grundrahmen der Infrastruktur und bilden deren Basis. Aus Sicht der Sicherheit gesehen sind gewisse Netzwerk-Komponenten die erste Hürde, welche überwunden werden müsste – egal ob dies von Innen oder Aussen geschieht.

Dabei ist in erster Linie wichtig, dass alle eingesetzten und operativen Komponenten erfasst werden. Mit dieser kompletten Liste kann überprüft werden, wie alt die jeweiligen Komponenten sind. Aufgrund des Alters lässt sich in vielen Fällen bereits aussagen, was für ein Sicherheits-Niveau vorhanden ist oder welches Niveau mit Wahrscheinlichkeit erreicht werden könnte. Falls die Komponente weniger als fünfjährig ist, macht die Kontrolle nach der installierten Firmware-Version Sinn.
Dabei sollte man im Hinterkopf behalten: Bei allen Firewalls mit direkter Internet-Anbindung sowie Netzwerk-Komponenten an exponierten Stellen (bspw. DMZ), sollte es zur Gewohnheit gehören, aktuelle Firmware-Versionen zeitnah aufzuspielen, um eine Verwundbarkeit auf aktuelle Bedrohungen möglichst klein zu halten.

Weiterer Beachtung muss den Sicherheit «Best-Practice» geschenkt werden. Keine neue Netzwerk-Komponente resp. um konfigurierte Komponente sollte ohne Berücksichtigung von Best-Practice Vorgaben produktiv geschalten werden. Solche Best-Practice Hinweise gibt es vielmals direkt von den verschiedenen Herstellern von Netzwerk-Komponenten für ihre spezifischen Produkte.
Allgemein gehaltene Sicherheits-Best-Practice können folgende Aussagen gemacht werden:

- Keine Standard-Kennwörter
- Keine Standard-Admins verwenden
- Keine Standard-IP verwenden
- Kennwörter regelmässig wechseln
- Privilegien-Trennung wo möglich nach Lese- und Schreibrechte unterscheiden (Least Privilege-Prinzip)
- Zugriffs-Kreis einschränken (physikalisch)
- Zugriffs-Daten nur privilegierten Personen zugänglich

3.2.1 Aufgabe: Beurteilung von Netzwerk-Komponenten

A1	Versuchen Sie in 2er-Gruppen für eines der folgenden Komponenten fünf bis zehn Sicherheits-Best-Practice Tipps oder Sicherheitsempfehlungen vom jeweiligen Hersteller ausfindig zu machen. Erläutern Sie dabei nicht allgemein gültige Grundsätze (siehe vorhergehende Seite), sondern suchen Sie spezifische Tipps und Grundregeln / Empfehlungen der verschiedenen Hersteller. Wenn Sie dabei wenige Punkte finden, führen Sie diese detailliert aus und beschreiben Sie, wie man diese konkret auf dem Produkt umsetzen kann.

Komponente	**Hersteller (Beispiel – nicht abschliessend)**
Firewall (Next Gen FW)	Fortinet, Sophos, Palo Alto, Barracuda usw.
Switch (Layer-3)	Cisco, D-Link, Netgear usw.
Router (Enterprise)	Cisco, Juniper usw.

Präsentieren Sie die Ergebnisse nach der Vorbereitungszeit in Form einer kurzen Präsentation (Dauer Präsentation: 6 bis 10 min.).

4 WLAN

Ein weiterer Sicherheitsaspekt bei einem Netzwerk stellt die Verbindung zum Netzwerk dar. Viele Endgeräte können zwischenzeitlich ohne Kabel in ein Netzwerk eingebunden werden, weshalb das Thema WLAN bei Netzwerksicherheitsfragen an Bedeutung gewinnt.

A1	Suchen Sie nach den aktuellen WLAN Standards. Wie lauten die Aktuellen? Was zeichnet diese aus? Welche Sicherheitseinstellungen unterstützen sie? Halten Sie Ihre Erkenntnisse im Kursnotizbuch fest.

5 Grundlagen von Remote Access-Techniken

Mit der VPN-Technologie werden private Daten über ein öffentliches Netz gesendet. Das ist die allgemein gehaltene Definition für den Begriff VPN.

Meistens ist mit der Bezeichnung VPN die IP-VPN Technologie gemeint. Dabei werden zwei entfernte Internet-Knotenpunkte über ein öffentliches Netz sicher miteinander verbunden. Der Datentransport erfolgt (teils) verschlüsselt über das Internet, dabei werden verschiedene Protokolle und Verfahren genutzt.

5.1 Kurzübersicht der VPN-Verfahren

- **IPSec** ist ein standardisiertes Verfahren, welches mehrere Sicherheitsaspekte beinhaltet, um die Datenübertragung zu schützen. Es kann zwei Netzwerke miteinander verbinden.

- **SSL-VPN** ist das VPN-Verfahren des Open-Source-Projekts OpenVPN. Hierbei wird zur Datenverschlüsselung das SSL (Secure Sockets Layer) resp. TLS (Transport Layer Security) Verschlüsselungsverfahren benutzt.

5.2 Authorisierungsmethoden

Auch für die Verschlüsselung und Authentifizierung können verschiedene Methoden benutzt werden. So können gemeinsame Schlüssel (PSK - **P**re**s**hared **K**eys) genutzt werden oder Zertifikate. Es können ebenso RSA- Schlüsselpaare benutzt werden, dies ist aber eher bei Gateway Verbindungen üblich.

- Bei einer PSK Authentifizierung handelt es sich um ein Kennwort, das beiden Verbindungspartnern bekannt ist und mit dem sie sich gegenseitig authentifizieren. Die Sicherheit dieser Methode ist somit abhängig von der Schlüsselstärke.

- Zertifikate des X.509 Standards, welcher ein asynchrones Kryptoverfahren darstellt, können ebenfalls als Authentifizierungsmethode benutzt werden. Die Zertifikate werden von einer vertrauenswürdigen Stelle (Zertifizierungsstelle) ausgestellt und signiert.

- Der Verbindungspartner identifiziert sich gegenüber dem anderen Teilnehmer mit seinem Zertifikat. Die Echtheit des Zertifikats kann die Gegenstelle mit dem Zertifikat der Zertifizierungsstelle (CA - Certification Authority) prüfen. Dieses Vorgehen wird in beide Richtungen der Verbindung angewendet. Die Methode ist zwar aufwendiger als das Preshared Key Verfahren, aber dafür auch sicherer.

- Die RSA Schlüsselpaar Methode ist ebenfalls ein asynchrones Kryptoverfahren. Hier besitzt jeder Verbindungspartner jeweils ein Schlüsselpaar, welches sich aus einem öffentlichen und einem privaten Schlüssel zusammensetzt. Der öffentliche Schlüssel wird gegenseitig ausgetauscht. Mit diesem wird die Verbindungsanfrage verschlüsselt. Nur der Besitzer des zugehörigen privaten Schlüssels kann diese Anfrage verifizieren, da so verschlüsselte Nachrichten nur mit dem privaten Schlüssel entschlüsselt werden können. Dieses Verfahren wird meistens nur bei Site-to-Site Verbindungen benutzt.

5.3 Verbindungsarten

Die Knotenpunkte können Hosts oder Netzwerk-Gateways sein. Damit unterscheidet man zwischen:

- Verbindungen von einem Host zu einem Gateway (sogenannte End-to-Site Verbindung)
- Verbindungen zwischen zwei Gateways (Site-to-Site Verbindungen).

	**VPN**	Informationen zu den Technologien resp. Protokollen.

5.4 Aufgaben

Um die verschiedenen Remote-Access Methoden und Verbindungsarten praktisch umzusetzen, werden Sie je ein End-to-Site sowie Site-to-Site VPN auf einer Sophos Firewall einrichten.

Um diese Konfiguration überhaupt durchzuführen, müssen die entsprechenden Firewalls von Grund auf eingerichtet werden. Dazu wird Ihnen der Kursleiter eine Einführung geben und die Grund-Konfiguration Schritt für Schritt erklären sowie die absolut notwendigen Einstellungen nennen.

5.4.1 Aufgabe: Next-Generation Firewall-Appliance einrichten

Die verschiedenen Gruppen richten Ihre Firewalls mit separaten Netzwerken ein, damit es für die nachfolgenden Aufgaben leichter fällt, den Überblick zu bewahren:

Gruppe	Netz
A	172.18.0.0 / 24
B	172.19.0.0 / 24
C	172.20.0.0 / 24
D	172.21.0.0 / 24
E	172.22.0.0 / 24
D	172.23.0.0 / 24
…	…

Stellen Sie in Ihrer 2er Gruppe die Einrichtung der Sophos Firewall Appliance gemäss Demonstration und Anweisungen vom Kursleiter sicher.

Nach diesen Ausführungen sollen die folgenden Punkte umgesetzt resp. sichergestellt sein:

1	Korrektes IP-Netz
2	Host-Name als FQDN definiert. Beispiel: *fw.uehlinger.tech*
3	Regions-Einstellung korrekt
4	Zeit-Server (NTP)
5	WAN-Konnektivität
6	"Default" Firewall-Regel überprüft
7	Neuer Administrator erstellt
8	Default Certificate generiert (Certificate Authority)
9	Update der Firmware
10	Backup der Systemkonfiguration erstellt

5.4.2 Aufgabe: Fernwartung für Firewall absichern

A1	Setzen Sie die nötigen Schritte um, welche Ihnen von Kursleiter demonstriert wurde. Sie enthalten Einstellungen im Bereich: - «Device access» Einschränkungen (Local services ACL) - «Admin console HTTPS port» - «Admin settings» - Benachrichtigungen sicherstellen

Zusätzlich stellen Sie folgendes Verhalten nach:

A2	Sichern Sie den Zugriff auf die Firewall Appliance so ab, dass Sie über den konfigurierten FQDN auf die Firewall zugreifen und im Browser keine Zertifikatswarnung mehr erhalten (und keine Sicherheits-Ausnahme generieren müssen!).

	**Firewall**	Informationen für die Umsetzungen.

5.4.3 Aufgabe: End-to-Site VPN einrichten

Diese Aufgabe entspringt dem Szenario, dass Mitarbeiter auch von zu Hause auf das Firmen-Netzwerk zugreifen möchten – zwecks Home-Office Möglichkeit, welche diese Mitarbeiter einmal pro Woche zur Verfügung haben.

A1	Erstellen Sie auf der Firewall fünf Benutzer, welche für VPN berechtigt werden. Fassen Sie diese Benutzer ebenfalls in einer Gruppe zusammen.
A2	Konfigurieren Sie SSL-VPN und testen Sie mit mindestens zwei Benutzern, ob der einfache Zugriff funktioniert.
A3	Konfigurieren Sie eine IPSec-Verbindung und testen Sie mit mindestens zwei Benutzern, ob der einfache Zugriff funktioniert. Beachten Sie, dass Sie den Sophos Connect Client über das Admin-GUI herunterladen können.
A4	Um weitere Tests nachvollziehbar abzulegen und kein Test-Szenario zu vergessen, erstellen Sie ein Testprotokoll, führen die Tests durch und halten die Ergebnisse fest.
Z1	Erstellen Sie eine dritte End-to-Site VPN Variante nach Ihrer Wahl. → Geben Sie vor der Konfiguration dem Kursleiter eine Begründung für die Wahl ab.
Z2	Testen Sie die dritte Variante ebenfalls mit mindestens zwei Benutzern und halten die Ergebnisse im Testprotokoll fest.

5.4.4 Aufgabe: Site-to-Site VPN einrichten

Eine Bau-Unternehmung mit Hauptsitz in Zürich eröffnet eine Zweigfiliale in Wetzikon und möchte diese an die bestehende Infrastruktur mittels VPN anbinden.

A1	Schliessen Sie sich mit einer anderen Gruppe zusammen.
A2	Konfigurieren Sie auf beiden Firewalls eine IPSec Site-to-Site Verbindung.
A3	Erweitern Sie das Testprotokoll um Site-to-Site Testfälle und testen anschliessend Ihre Umsetzung.
A4	Erstellen Sie als Alternative eine SSL Site-to-Site Verbindung.
A5	Erweitern Sie nochmals das Testprotokoll und testen die zweite Variante ebenfalls in den Gruppen.
Z1	Arbeiten Sie gemäss Kap. 13 mit einer anderen Virtual Appliance.

	**VPN**	Informationen für die Umsetzungen.

6 Sicherheit für den WAN-Zugriff

Die einst gängige Philosophie, dass man jeglichen Verkehr nach Aussen erlaubt, ist heute in den wenigsten Fällen sorgenfrei umsetzbar. Zu gross ist die Gefahr, dass Seiten oder Dienste aufgerufen resp. benutzt werden, welche selber durch Schadsoftware oder Viren verseucht sind, oder mit Werbungen usw. auf dubiose Seiten und Dienste verwiesen wird.

Sicherheit beginnt von Innen. Damit man den Zugriff von Intern nach Aussen steuern, regulieren und kontrollieren kann, sind heute Werkzeuge gefordert, welche alle diese Anforderungen erfüllen.

Desweitern möchte man auch im Griff haben, auf welche Inhalte und Dienste die Mitarbeiter überhaupt zugreifen können. Als Beispiel können hier die Seiten von sozialen Medien erwähnt werden, welche für einen System Engineer oder Projektleiter meist überhaupt nicht relevant sind, für Mitarbeiter von Marketing oder Web-Entwicklung aber schon.

In den Zeiten wo sich Next-Generation Firewalls grosser Beliebtheit erfreuen, ist es nicht mehr nötig, für oben genannte Absicherungen jeweils eigene Security Appliances zu betreiben. Damit sinkt die Hemmschwelle, solche Filterungen zu konfigurieren und einzuschalten. Auch wenn die Konfiguration rasch etwas komplexer werden kann und eine vorgängige Planung über die Filter-Einstellungen entscheidend ist, soll das nicht als Ausrede dienen – vor allem nicht ab einem KMU Grössenbereich.

6.1.1 Aufgabe: Virtual Appliance einrichten

Für diesen Aufgabenblock werden wir die virtuelle Umsetzung eines Sophos OS benutzen. Als Hypervisor benutzen wir VMware Workstation Player.

Stellen Sie wieder sicher, dass die Grundkonfiguration der Firewall wie in Kap. 5.4.1 und 5.4.2 umgesetzt ist.

6.1.2 Aufgabe: Web-Filterung einsetzen

Jetzt soll die Grundeinrichtung von dem Web-Filter Modul in Angriff genommen werden.

Folgende Vorgaben sind gegeben und sollen auf der Virtual Appliance umgesetzt werden:

Nr.	Vorgabe	Zeit-Steuerung
1	https-Seiten werden entschlüsselt und geprüft.	keine
2	Social-Media Inhalte sind gesperrt	Ganztags
3	Video- und Streaming-Portale wie Youtube, Netflix sind gesperrt	Ganztags
4	News-Portale sind gesperrt	08:00 bis 17:00
5	Kein Zugriff auf Cloud-Dienste wie OneDrive, iCloud, Dropbox usw.	Ganztags

7 Datenverkehr analysieren

Im Infrastruktur-Umfeld ist man oftmals mit Fragen konfrontiert, was läuft im Netzwerk überhaupt für Datenverkehr ab. Ist das vorwiegend geschäftliche Kommunikation oder ist doch der Anteil an privater Nutzung unverhältnismässig hoch?

Für die Beantwortung von solchen Fragen stehen einerseits Netzwerk-Monitor Systeme zur Verfügung, welche andauernd den Verkehr oder gewisse Bereiche davon mitschneiden. Es kann aber auch vorkommen, dass Sie kurzfristig für ein Problem oder Frage im Datenverkehr Stellung nehmen müssen. Für solche Zwecke eignen sich meistens andere Werkzeuge wie bspw. Sniffer.

F1	Was für Erfahrungen haben Sie mit Netzwerk-Monitor-Systemen oder Sniffer bereits gemacht und wozu?
F2	Anhand von welchen Kriterien können Sie eine Aussage über die Sicherheit des Datenverkehrs treffen?
A1	Wählen Sie ein Sniffer-Tool für die folgende Aufgabe aus.
A2	Schneiden Sie mit dem Sniffer-Tool den Verkehr mit, welchen Sie über die Virtual Appliance generieren. Legen Sie den Fokus auf das Verhalten, wenn Verkehr wegen einer Firewall-Regel oder wegen der Web-Filterung geblockt wird. Was sind Ihre Erkenntnisse dazu?
A3	**Hilfestellung** – Funktionsweise SSL/TLS Untersuchen Sie mit Qualys folgende Webseiten: • www.google.com • www.r-au.ch • Webseite von Ihrem Verein/Schule/… • Webseite von Ihrer virtuellen Sophos Appliance Wie beurteilen Sie die untersuchten Webseiten hinsichtlich der Sicherheit des Datenverkehrs?

8 Intrusion Prevention / Detection System

Das Angriffsschutzsystem (Intrusion Prevention System, IPS) erkennt Angriffsversuche anhand eines meist signaturbasierten Regelwerks. Das System analysiert den gesamten Datenverkehr und blockiert Attacken automatisch, bevor diese das lokale Netzwerk erreichen. Das bereits vorhandene Regelwerk und die Angriffsmuster werden durch die Pattern-Updates-Funktion aktualisiert. Neue IPS-Angriffs-Pattern-Signaturen werden automatisch als IPS-Regeln in das Regelwerk importiert.

Im Gegensatz dazu ist ein Intrusion Detection System bzw. Angrifferkennungssystem nur ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Netzwerk gerichtet sind. Erkannte Angriffe werden meistens in Log-Dateien gesammelt und dem Benutzer oder Administrator mitgeteilt.

8.1.1 Aufgabe: Umsetzung IPS auf Sophos

Die Einstellungen für Intrusion Detection System auf der Sophos resp. auf der Virtual Appliance sind grundsätzlich nach Regel-Gruppen aufgebaut und daneben gibt es die Möglichkeiten für DoS-Verhinderung und Anti-Portscan.

A1	Richten Sie gemäss den Anweisungen vom Kursleiter das IPS für bestimmte Regel-Gruppen sowie andere Einstellungen ein.

	IPS	Hier finden Sie die Anforderungen.

8.1.2 Aufgabe: Umsetzung IPS als eigenständiger Service

Neben der integrierten Art auf einer Next-Generation Firewall können wir IPS auch als eigenständigen Service einrichten und im Netzwerk integrieren.

Zur Auswahl stehen weitverbreitete Network IDS / IPS (NIDS). Das primäre Ziel ist, dass jeder von Ihnen ein NIDS virtuell einrichten kann und so konfiguriert, dass sie den Anforderungen der vorhergehenden Aufgabe entspricht (soweit möglich).

	IPS	NIDS

9 Beurteilung von aktuellen Exploits

Wenn von Netzwerksicherheit gesprochen wird, muss man sich auch mit der aktuellen Sicherheits-Lage befassen. Die Meldungen von Exploits und anderen Sicherheits-Risiken im Bereich IT-Infrastruktur lassen nicht nach.

In diesem Zusammenhang ist es wichtig, dass man regelmässig überprüft, was es für neue Sicherheits-Massnahmen von Seiten Hersteller von IT Sicherheits-Produkten gibt. Um Sicherheits-Massnahmen zu verstehen und nachvollziehen kann, ist eine Auseinandersetzung mit den Exploits und anderen Bedrohungen sehr wichtig.

	Cybercrime-Bundeslage-bild	Cybercrime-Bundeslagebild

A1	Lesen Sie das Cybercrime Bundeslagebild vom deutschen Bundeskriminalamt durch.
A2	Beurteilen Sie in 2er Gruppen einen aktuellen Exploit und recherchieren Sie nach dessen technischen Eigenheiten. Suchen Sie ebenfalls nach Praxis-Beispielen von solchen Verseuchungen und deren Auswirkung auf den Betrieb der Infrastruktur. Beispiele für Ransomware-Exploits: - GoldenEye - WannaCry - Petya - Linux-Varianten? Halten Sie die zwei Punkte in Form einer Präsentation fest. Präsentationsdauer: 6 bis 10 min

10 Überwachen

In Ihrer bisherigen Ausbildung haben Sie Möglichkeiten kennen gelernt, wie Sie mit einem Monitoring Tool Systemkennzahlen überwachen können. Ebenfalls haben Sie festgestellt, dass Ereignisse in Logs gespeichert werden.

10.1 Aufgaben

10.1.1 syslog-ng aktivieren und konfigurieren

Um Log-Aktivitäten und deren Auswertung nicht nur lokal auf einer Netzwerk-Komponente zu speichern, eignet sich die Auslagerung resp. die zentrale Ablage von jeglichen Log-Ansammlungen auf einem Log-Server.

Der syslog Server-Dienst auf Linux-Systemen ist dazu sehr gut geeignet und kann individuell konfiguriert werden.

A1	Installieren Sie als Grundlage für syslog einen aktuellen virtuellen Ubuntu-Server auf Ihrem Client.
A2	Aktivieren Sie syslog-ng auf dem Ubuntu Server.
A3	Konfigurieren Sie die Firewall so, dass Logs ab jetzt zum syslog Server gehen.
A4	Sicherstellung, dass definierte Firewall-Logs als eigene Log-Datei auf dem syslog-Server abgelegt werden.
A5	Testen Sie Ihre Umsetzung und erstellen Sie dazu ein Testprotokoll

10.1.2 SNMP einrichten

A1	Installieren Sie als Grundlage für das Monitoring mit SNMP einen aktuellen virtuellen Windows-Server auf Ihrem Client.
A2	Installieren Sie die kostenfreie Testversion von PRTG.
A3	Konfigurieren Sie Ihr Monitoring so, damit Sie sinnvolle Werte der Firewall überwachen können.
A4	Testen Sie Ihre Umsetzung und erstellen Sie dazu ein Testprotokoll.

	**Überwachen**	Informationen für die Umsetzungen.

11 Weitere Virtual Appliances kennen lernen

Z1	Machen Sie auf der gewählten Virtual Appliance die Grundkonfiguration.
Z2	Konfigurieren Sie auf der gewählten Virtual Appliance die Firewall-Regeln im gleichen Muster wie auf der Sophos.
Z3	Richten Sie eine End-to-Site VPN-Verbindung ein.
Z4	Konfigurieren Sie zu zweit ein Site-to-Site VPN.
Z5	Konfigurieren Sie auf der gewählten Virtual Appliance die Web Filterung nach gleicher Vorgabe wie auf der Sophos.
Z6	Konfigurieren Sie IPS auf der Firewall.