OpenVPN-Zugang für Mitarbeiter der Learn-IT GmbH einrichten

Fach	IT-Systeme
Lernfeld	LF 9: Netzwerke und Dienste bereitstellen
Querverweise zu weiteren Lernfeldern des Lehrplans	LF 4: Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen
Zeitrahmen	10 Unterrichtsstunden (5 Doppelstunden)
Benötigtes Material	Windows-Arbeitsplatzrechner mit Internetzugang und Administrationsrecht, optional als virtuelle Maschinen, Aktuelle Version der quelloffenen VPN-Software OpenVPN (openvpn.net), Netzwerklabor oder schulische Netzwerkinfrastruktur, Flipcharts oder DIN A3-Papier, Medienkoffer, Optional: aktuelle Version der quelloffenen TLS-Suite OpenSSL (openssl.org), Optional: Virtualisierungssoftware und den schulischen Laborbedingungen angepasste, durch die Lehrkraft vorbereitete virtuelle Maschinen, Netzwerkmonitor (tcpdump, Wireshark etc.)

Kompetenzerwartungen

Die Schülerinnen und Schüler …

- ... beraten Kunden und Kundinnen auch unter Einbezug fremdsprachiger Quellen im Hinblick auf Anforderungen an die IT-Sicherheit und an den Datenschutz. (Medienkompetenz)
- ... bewerten externe IT-Ressourcen, wählen sie aus und integrieren sie in ein IT-System. (Anwendungs-Know-how)
- … installieren Systemkomponenten und Netzwerkbetriebssysteme, passen sie an und konfigurieren sie. (Anwendungs-Know-how)
- … unterscheiden Netzwerkkonzepte für unterschiedliche Anwendungsgebiete. (Informatische Grundkenntnisse)

- … legen Sicherheitsmechanismen, insbesondere Zugriffsmöglichkeiten und -rechte, fest und implementieren diese. (Informatische Grundkenntnisse)

Aufgabe

1. **Orientieren:**

   1 Unterrichtsstunde

   Nachdem sich die Geschäftsführung der Learn-IT GmbH über unterschiedliche VPN-Konzepte informiert hat, beabsichtigt sie, ihren Schulungsmitarbeitern einen OpenVPN-Zugang zur Verfügung zu stellen, damit diese bei Inhouse-Schulungen auf aktuelle Kursmaterialien von außerhalb zugreifen können. Die Schülerinnen und Schüler erhalten den Auftrag, diesen OpenVPN-Zugang zu realisieren. Dafür erhalten sie von der Lehrkraft die vorformulierten Anforderungen an das gewünschte End-to-Site-VPN, das Daten verschlüsselt übertragen und zusätzlich Authentisierung und Authentifizierung mittels X.509-Zertifikaten ermöglichen soll. Anhand dieser Anforderungen erarbeiten sie in Einzelarbeit zum Beispiel in Form eines Mindmaps stichpunktartig Argumente, die die Entscheidung der Firmenleitung der Learn-IT GmbH unterstützen, indem sie auch fremdsprachige, von der Lehrkraft vorbereitete Informationsquellen nutzen.

2. **Informieren:**
   2 Unterrichtsstunden

   Auf Grundlage der in der Orientierungsphase gesammelten Argumente für ein quelloffenes VPN informieren sich die Schülerinnen und Schüler mittels einer kurzen Internet-Recherche in Einzelarbeit über Typ und Betriebsart des zu realisierenden VPN's (End-to-Site-Verbindung im Routing-Mode), die für diese Betriebsart nötigen Endpunkte (Client und Gateway) sowie die dafür erforderlichen Software-Produkte bzw. -Quellen (openvpn.net). Sie recherchieren grundlegende Informationen zum VPN-Tunneling unter Nutzung privater und öffentlicher IPv4-Adressräume sowie den zugehörigen virtuellen Netzwerkgeräten (TAP- bzw. TUN-Devices), die über spezielle Treiber für die VPN-Nutzung bereitgestellt werden. ***Optional:*** *Die Schülerinnen und Schüler ergänzen die von ihnen gesammelten Informationen um Möglichkeiten der VPN-Verschlüsselung auf den OSI-Schichten 5 (Session) und 7 (Application) mittels quelloffener Software wie OpenSSL (openssl.org), mit der die für eine TLS-Verschlüsselung unter Bereitstellung*

von X.509-Zertifikaten erforderliche kryptographische Infrastruktur realisiert werden kann.

3. Planen:

1 Unterrichtsstunde

Das in Orientierungs- und Informationsphase erarbeitete Grundlagenwissen nutzen die Schülerinnen und Schüler für die skizzenhafte Ausarbeitung eines VPN-Szenarios (Abschnitt "Schülerlösungen") in Partnerarbeit, dass die vom Kunden beabsichtigte Nutzung des Mitarbeiters -VPN's schematisch darstellt. Im Anschluss übersetzen sie dieses Szenario auf die an der Schule vorhandenen Laborbedingungen. Dafür ergänzen sie ihr VPN-Szenario mit den entsprechenden IPv4-Adressen, so dass es in der nachfolgenden Durchführungsphase als Grundlage für Konfigurationen und - wenn nötig auch unter Zuhilfenahme virtueller Maschinen - Schnittstellenadressierung dienen kann. ***Optional:*** *Sollen die VPN-Mitarbeiterzugänge (den Anforderungen entsprechend) mittels Hybridverschlüsselung über X.509-Zertifikate abgesichert werden, erstellen die Schülerinnen und Schüler zusätzlich eine Übersicht über die dafür notwendige Zertifikatehierarchie und die zugehörigen Zertifikateinformationen sowie die entsprechenden Speicherorte auf VPN-Gateway und -Client.*

4. **Durchführen:**

5 Unterrichtsstunden

In der Durchführungsphase setzen die Schülerinnen und Schüler ihre Partnerarbeit fort. Vor der Realisierung des geplanten bzw. auf die Schulinfrastruktur abgebildeten VPN-Szenarios laden sie die erforderlichen Softwarepakete herunter und installieren diese (openvpn.net, ***optional:*** *openssl.org*). Dabei muss bei Windows-Systemen die Installation der TUN-/TAP-Devices zugelassen und danach in den Netzwerkeigenschaften geprüft werden. Das neu installierte TAP-Device muss im Anschluss mit der jeweils verwendeten physischen LAN- oder WLAN-Schnittstelle gebrückt werden. Dafür beide Adapter (TAP- und physisches Device) markieren und nach Klick auf die rechte Maustaste brücken (Kontextmenü: "Verbindungen überbrücken"). Daraufhin erscheint ein neuer Netzwerkadapter "Netzwerkbrücke" in den Netzwerkeigenschaften.

Um sich nach der Installation mit der Bedienung von OpenVPN auf der Kommandozeile vertraut zu machen, nehmen die Schülerinnen und Schüler eine erste unverschlüsselte VPN-Verbindung in Betrieb. Ein Schülerrechner repräsentiert dabei das VPN-Gateway, der andere den VPN-Client. Wie im VPN-Szenario (Abschnitt "Schülerlösungen") dargestellt, verfügt das Gateway über mindestens drei IPv4-Adressen, eine private Intranet-Adresse (z.B. 192.168.2.1/24), eine öffentliche, dem Client bekannte Internet-Adresse (im Schulnetz beispielsweise simuliert über die schulinterne, über DHCP vergebene IPv4-Adresse, z.B. 172.16.2.145/16) sowie eine aus einem separaten Adressraum stammende private IPv4-Adresse (z.B. 10.0.0.10/24) für den Abschluss des VPN-Tunnels. Der Client nutzt die ihm meist über DHCP öffentlich zugewiesene IPv4-Adresse (auch hier kann die schulinterne private DHCP-Adresse genutzt werden, z.B. 172.16.2.165/16) und eine aus demselben Adressraum wie beim Gateway stammende private Adresse als Tunnelabschluss (z.B. 10.0.0.20/24). OpenVPN arbeitet standardmäßig auf UDP- und TCP-Port 1194. Bei Windows-Systemen wird der Benutzer beim Start der OpenVPN-Verbindung normalerweise von der internen Firewall Funktion aufgefordert, den Zugriff auf diesen Port zuzulassen. ***Hinweis:*** *Für die Simulation des VPN-Tunnels kann auf den Durchgriff vom Inter- ins Intranet verzichtet werden. Für schnelle Schülerinnen und Schüler ist die Realisierung dieses Durchgriffs schon im Anschluss an dieses illustrierende Beispiel jedoch mit Sicherheit ein Erfolgserlebnis!*
Mit den folgenden Kommandozeilenbefehlen kann eine erste ungesicherte Testverbindung zwischen VPN-Client und -Gateway aufgebaut werden:

VPN-Gateway:

```
openvpn --remote 172.16.2.165 --dev tun0 --ifconfig 10.0.0.10 10.0.0.20 --verb 5
```

VPN-Client:

```
openvpn --remote 172.16.2.145 --dev tun0 --ifconfig 10.0.0.20 10.0.0.10 --verb 5
```

Ob die Verbindung zustande gekommen ist, können die Schülerinnen und Schüler an der Meldung Initialization Sequence Completed erkennen. Danach können sie die Verbindung durch gegenseitiges Anpingen der VPN-IPv4-Adressen (10.0.0.10 bzw. 10.0.0.20) testen.

War dieser erste Test erfolgreich, legen die Schülerinnen und Schüler anhand einer von der Lehrkraft zur Verfügung gestellten Vorlage einfache OpenVPN-Konfigurationsdateien (test_gateway.ovpn und test_client.ovpn, Abschnitt "Schülerlösungen") an, in die sie die Parameter der funktionierenden Testverbindung

übertragen. Mit diesen Dateien als OpenVPN-Übergabeparameter testen die Schülerinnen und Schüler die VPN-Verbindung mit folgenden Kommandozeilenbefehlen erneut:

VPN-Gateway:

```
openvpn --config c:\Programme\OpenVPN\config\test_gateway.ovpn
```

VPN-Client:

```
openvpn --config c:\Programme\OpenVPN\config\test_client.ovpn
```

Soll die End-to-Site-Verbindung (auch: Client-to-Network-Verbindung) - wie in der Kundenanforderung vorgesehen - TLS-basiert mittels X.509-Zertifikaten und den zugehörigen Verschlüsselungs- und Authentisierungsmechanismen abgesichert werden, erstellen die Schülerinnen und Schüler eine reduzierte Zertifizierungsstelle (hier unter Zuhilfenahme des OpenVPN-Tools Easy-RSA) und legen zusätzlich die erforderlichen privaten und öffentlichen Schlüssel sowie Diffie-Hellman-Parameter für den Austausch des pro VPN-Sitzung nötigen Session-Keys an. Die Zertifizierungsstelle (Certification Authority, CA) wird auf dem VPN-Gateway unter Benutzung der OpenVPN-Kommandozeilenbefehle angelegt:

```
C:>cd .\Programme\OpenVPN\easy-rsa
C:\Programme\OpenVPN\easy-rsa>init-config.bat
```

Die als Ergebnis erzeugte Dateivorlage vars.bat (Abschnitt "Schülerlösungen") muss von den Schülerinnen und Schülern angepasst werden. Nach dieser Anpassung wird die neue CA initialisiert:

```
C:\Programme\OpenVPN\easy-rsa>vars.bat
C:\Programme\OpenVPN\easy-rsa>clean-all.bat
```

Jetzt können privater Schlüssel und Stammzertifikat der CA erzeugt werden, die anschließend als ca.key (priv. Schlüssel) und ca.crt (Stammzertifikat) im Unterverzeichnis keys auf dem VPN-Gateway liegen sollten. Gleichzeitig werden die Diffie-Hellman-Parameter für den Austausch des Session-Keys angelegt:

```
C:\Programme\OpenVPN\easy-rsa>build-ca.bat
C:\Programme\OpenVPN\easy-rsa>build-dh.bat
```

Das Stammzertifikat wird nun von den Schülerinnen und Schülern genutzt, um Schlüssel sowie Zertifikate für Client und Gateway zu generieren:

```
C:\Programme\OpenVPN\easy-rsa>build-key-server.bat gateway
C:\Programme\OpenVPN\easy-rsa>build-key.bat client
```

Schlüssel und Zertifikate können im Sinne der Übersichtlichkeit der Verwaltung in PKCS#12-Dateien zusammengefasst werden:

```
C:\Programme\OpenVPN\easy-rsa>build-key-pkcs12.bat gateway
C:\Programme\OpenVPN\easy-rsa>build-key-pkcs12.bat client
```

Die neu angelegten PKCS#12-Dateien müssen danach auf dem jeweiligen Endgerät im Verzeichnis C:\Programme\OpenVPN\config\certs abgelegt werden. An dieser Stelle sollten die Schülerinnen und Schüler dafür sensibilisiert werden, dass die Weitergabe der PKCS#12-Datei an den Client für die Vertraulichkeit des privaten Schlüssels und des zugehörigen Zertifikats sicherheitskritisch ist (*LF 4*).

Die Schülerinnen und Schüler schließen die Durchführungsphase ab, indem sie ein Multiclient-VPN realisieren, das mehr als eine End-to-Site-Verbindung von Client zu VPN-Gateway ermöglicht. Das Gateway, das im einfachsten Fall auch das Default-Gateway des Intranets der Learn-IT GmbH sein sollte, dient dabei als DHCP-Server für das virtuelle private Netzwerk. In dieser Funktion weist es den mobilen Clients IPv4-Adressen zu und speichert diese Zuordnung in der Textdatei ipp.txt, um bekannten Clients beim Neuaufbau einer Verbindung jeweils dieselbe IPv4-Adresse zuweisen zu können. Die VPN-Verbindungen sollen außerdem verschlüsselt und über die im vorherigen Arbeitsschritt erstellten Zertifikate authentifiziert arbeiten. Die Schülerinnen und Schüler passen dafür in Partnerarbeit von der Lehrkraft vorgegebene OpenVPN-Konfigurationsdateien (client.ovpn und gateway.ovpn, Abschnitt "Schülerlösungen") an das in der Planungsphase erarbeitete VPN-Szenario an. ***Hinweis:*** *Erforderliche fachliche Informationen können den Kommentaren in den OpenVPN-Konfigurationsdateien entnommen werden.* Mit Hilfe der angepassten Konfigurationsdateien nehmen die Schülerinnen und Schüler das Multiclient-VPN in Betrieb (Vorgehensweise s.o.: Testverbindung).

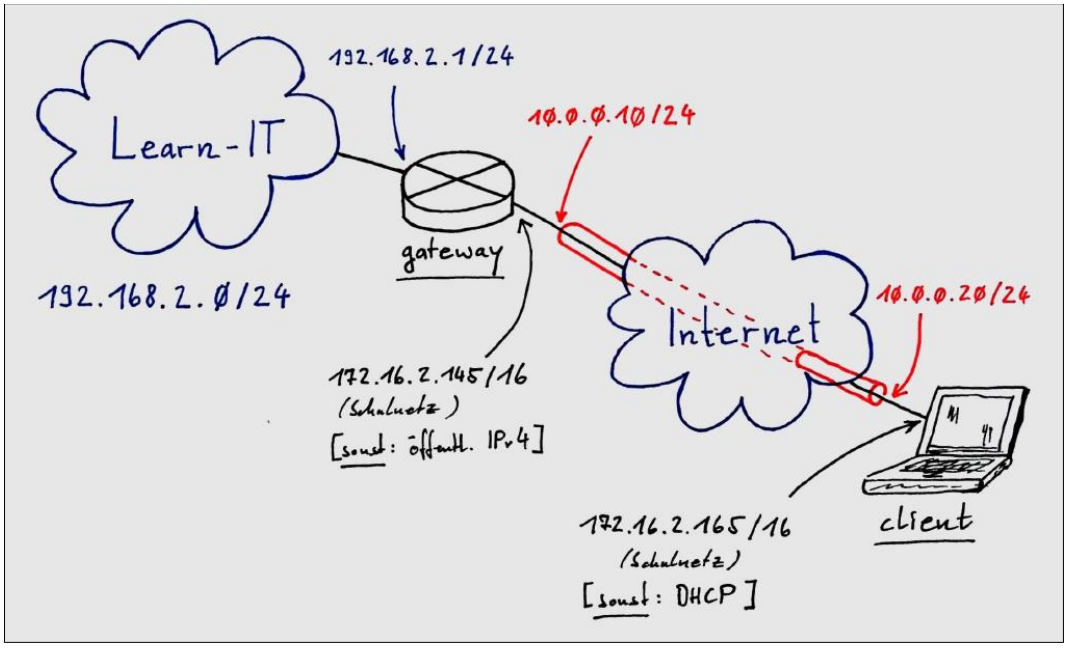
5. **Kontrollieren und Bewerten:**

1 Unterrichtsstunde

Die Schülerinnen und Schüler beenden die dargestellte Lernsituation in Partnerarbeit, indem sie unter Zuhilfenahme eines gängigen Netzwerk-Monitoring-Tools sowohl die unverschlüsselte als auch die abgesicherte Verbindung zwischen VPN-Client und -Gateway in jeweils einem Capture-Ergebnis darstellen. Dafür ist ein Konnektivitätstest bzw. eine Routenverfolgung mittels Kommandozeilentools (ping, tracert etc.) in der Regel ausreichend. Natürlich müssen beim Mitschnitt über die eingesetzten Tools die entsprechenden IPv4-Zieladressen angesprochen werden. Beim Test vom Client zum Gateway nutzen die Schülerinnen und Schüler deshalb für die unverschlüsselte Verbindung die "öffentliche" IPv4-Adresse des Gateways (hier: 172.16.2.145), beim Test der eigentlichen VPN-Verbindung die private, als Tunnelabschluss eingesetzte Gateway-Adresse (hier: 10.0.0.1). Danach diskutieren sie eines der Schülerergebnisse im Klassenplenum. Dabei kann auf entstehende Fragen gemeinsam mit der Lehrkraft eingegangen werden.

Beispiele für Produkte und Lösungen der Schülerinnen und Schüler

Planen: VPN-Szenario



Durchführen: `test_client.ovpn` und `test_gateway.ovpn`

test_client.ovpn:

```
# IP address of remote host (gateway)
remote 172.16.2.145

# Use the TUN device for routing mode
dev tun0

# Specify local and remote VPN addresses.
# 10.0.0.20 is the local VPN IP address and
# 10.0.0.10 is the remote VPN IP address.
# Swap the order of the ifconfig addresses on the remote machine.
ifconfig 10.0.0.20 10.0.0.10

# Moderate verbosity for debugging
verb 5

```

test_gateway.ovpn:

```
# IP address of remote host (client)
remote 172.16.2.165

# Use the TUN device for routing mode
dev tun0

# Specify local and remote VPN addresses.
# 10.0.0.10 is the local VPN IP address and
# 10.0.0.20 is the remote VPN IP address.
# Swap the order of the ifconfig addresses on the remote machine.
ifconfig 10.0.0.10 10.0.0.20

# Moderate verbosity for debugging
verb 5

```

Durchführen: Auszug aus `vars.bat`

```
rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=DE
set KEY_PROVINCE=BY
set KEY_CITY=Erlangen
set KEY_ORG="Learn-IT GmbH"
set KEY_EMAIL=info@learn-it.de
set KEY_CN=gateway
set KEY_NAME=gateway
set KEY_OU=Headquarters
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234

```

Durchführen: `client.ovpn` und `gateway.ovpn`

client.ovpn:

```
# Use config-directory
cd c:\\Programme\\OpenVPN\\config

# VPN gateway IP
remote 172.16.2.145

# Use the TUN device for routing mode
dev tun0

# Port and protocol
port 1194
proto udp

# Packet sizes
tun-mtu 1500
fragment 1300
mssfix

# VPN client mode
pull

# Authentication client
tls-client
auth SHA1

# Session cipher
cipher AES-256-CBC

# Certificate
pkcs12 certs\\client.p12

# Activate compression
comp-lzo yes

# Debug level
verb 3

```

gateway.ovpn:

```
# Use config-directory
cd c:\\Programme\\OpenVPN\\config

# Use the TUN device for routing mode
dev tun0

# Port and protocol
port 1194
proto udp

# Packet sizes
tun-mtu 1500
fragment 1300
mssfix

# VPN gateway mode - server for VPN 10.0.0.0/24
mode server
server 10.0.0.0 255.255.255.0
keepalive 10 60

# VPN client address pool (server address: 10.0.0.1/24)
ifconfig-pool-persist ipp.txt

# Push route to mobile client for intranet access
push "route 192.168.2.0 255.255.255.0"

# Authentication server
tls-server
auth SHA1

# Diffie Hellman params
dh dh1024.pem

# Session cipher
cipher AES-256-CBC

# Certificate
pkcs12 certs\\gateway.p12

# Activate compression
comp-lzo yes

# Debug level
verb 3

```

Hinweis zum Unterricht

Ist es innerhalb der schulischen IT-Infrastruktur nicht möglich, Schülerinnen und Schüler mit Administrationsrechten für die benötigten Endgeräte auszustatten, können VPN-Client und -Gateway auch als virtuelle Maschinen emuliert werden. Für deren Inbetriebnahme muss unter Umständen zusätzlich Unterrichtszeit eingeplant werden. VPN-Tunneling bedeutet nicht unbedingt die verschlüsselte und authentifizierte Übertragung von Daten, sondern kann auch unverschlüsselt und nicht authentifiziert erfolgen. Das hier beschriebene Beispiel kann reduziert unterrichtet werden, wenn auf Verschlüsselung und Authentifizierung unter Verwendung von Zertifikaten verzichtet wird. Das Konzept eines VPN's mit der hier beschriebenen Betriebsart Routing-Mode (bei IPsec: Transport-Mode) kann trotzdem hinreichend erarbeitet werden. Die Kombination von VPN-Betrieb und kryptographischen Verfahren ist in der Praxis sinnvoll. Beide bedingen einander aber nicht. Im hier beschriebenen illustrierenden Beispiel wird das VPN auf Windows-Systemen implementiert. Sind entsprechende Linux-Kenntnisse vorhanden, empfiehlt sich jedoch der Einsatz von Linux-Systemen für VPN-Gateway und -Client, da dann die Kommandozeile sowohl für OpenVPN als auch für OpenSSL durchgängig angewendet werden kann. Denkbar ist natürlich auch der gemischte Einsatz beispielsweise eines Linux-Systems als VPN-Gateway und eines Windows-Systems als VPN-Client.

Querverweise zu anderen Fächern / Fachrichtungen

Grundlagenwissen zu kryptographischen Methoden (symmetrische/asymmetrische bzw. Hybrid-Verschlüsselung, Hashwerte und Zertifikate, Authentisierung und Authentifizierung) sollte bereits im ersten Ausbildungsjahr (10. Jgst.) in Lernfeld 4 zumindest auf theoretischer Ebene gelegt worden sein.

Quellen- und Literaturangaben

- OpenVPN, OpenVPN Inc., 7901 Stoneridge Drive, Suite 540, Pleasanton CA, United States 94588, https://openvpn.net, (Zugriff 30-05-2020. 15:03 MEZ)
- OpenSSL, OpenSSL Software Foundation, Newark DE 19711 USA , https://www.openssl.org, (Zugriff 30-04-2020. 16:19 MEZ)
- Notepad++, Don Ho, https://notepad-plus-plus.org, (Zugriff 09-04-2020. 15:50 MEZ)