

UNIT 3 - Woche 5 - Sicherheit auf Geschäftsreisen - Verschlüsselung von E-Mails

Verschlüsselung von E-Mails

In diesem Modul lernen Sie, wie Sie Ihre E-Mail-Nachrichten verschlüsseln.

In diesem Beispiel wurden der kostenlose E-Mail-Client Thunderbird und zwei Test-E-Mail-Konten verwendet

Fast alle E-Mails, die Benutzer normalerweise senden/empfangen, sind unverschlüsselt

Sie müssen die E-Mail-Verschlüsselung in den Kontoeinstellungen aktivieren

Zu diesem Zweck müssen Sie zwei Schlüssel erstellen: einen privaten und einen öffentlichen

Nachdem Sie das Schlüsselpaar erstellt haben, müssen Sie den PUBLIC-Schlüssel an Ihre Empfänger senden.

Mit dem PUBLIC-Schlüssel können Ihre Empfänger E-Mails verschlüsseln, die nur Sie lesen können.

Senden Sie niemals Ihren PRIVATEN Schlüssel

Zur Verschlüsselung muss der Empfänger Ihren PUBLIC-Schlüssel importieren

Importieren Sie die empfangene Datei mit dem PUBLIC-Schlüssel

Nach dem Import müssen Sie diesen Schlüssel verifizieren

Für die Verschlüsselung müssen Sie die Option "Sicherheit" und "Verschlüsselung erforderlich" wählen.

Wenn alles in Ordnung ist, ist die empfangene Nachricht verschlüsselt.

Wenn Sie Nachrichten an Ihren Empfänger verschlüsseln möchten, sollten Sie seinen öffentlichen Schlüssel importieren.

Ohne den PRIVATEN Schlüssel kann niemand sehen, was in der E-Mail steht.

Senden Sie niemals Ihren PRIVATEN Schlüssel

Machen Sie immer eine Kopie Ihres PRIVATEN Schlüssels

Ohne PRIVATE-Schlüssel werden Ihre E-Mail-Nachrichten immer verschlüsselt und gehen verloren

UNIT 3 – Week 5 - Security at business trips - VPN

VPN

In this module you will learn how safely connect to your enterprise internal computer network

In this example, the free RADMIN VPN application was used

This is internal website that can be only viewed in company network

We can see that this PC is in the internal network

This PC is connected to the outside network and has no connection to the company network

This PC can't connect to the internal webpage

To create this possibility you can use RADMIN VPN

In your internal network computer choose Create Network

For safely enter unique network name and safe password

In the remote PC all that's left is to enter the network name and password

Now you can try connect to the internal webpage, but first you must check what IP address it have

You can read Enterprise server VPN new IP in RADMIN VPN application

Now you can connect to the internal network

You can also view shared folders in your internal network

To end this connection just disable Network

After disabling connection you can't connect to your internal network

UNIT 3 – Week 5 - Security at business trips – Wireless network security

Wireless network security

In this module you will learn which wireless network security is more safe

It's not recommend to connect to the "Open" Wireless network

Your connection can be monitored by hackers

Attempting to connect to the more secure network type "WEP"

It took only about 1 hour to break any WEP password

Attempting to connect to the secure network type "WPA2"

Beneath the name of WIFI connection is type of connection "Secured"

In the setting the type of connected Wireless security is WPA2-Personal

Hackers can use brute-force method to decipher your password

For this purpose they create dictionary with all variations of characters

Then how long will it take to crack the password?

It took about 47 minutes to crack this password

Then how secure Wireless Network?

Always use passwords that:

- 1) Contain at least 9 characters
- 2) Contain at least one Upper case and Lower case character
- 3) Contain at least one number
- 4) Contain at least one special character like: "!"