

UNITÀ 3 - Settimana 5 - Sicurezza durante i viaggi di lavoro - Crittografia della posta elettronica

Crittografia delle e-mail

In questo modulo imparerete a crittografare i vostri messaggi di posta elettronica.

In questo esempio sono stati utilizzati il client di posta elettronica gratuito Thunderbird e due account di posta elettronica di prova.

Quasi tutte le e-mail che l'utente invia/riceve abitualmente sono in chiaro.

È necessario abilitare la crittografia delle e-mail nelle impostazioni dell'account.

A questo scopo è necessario creare due chiavi: una privata e una pubblica.

Dopo aver creato le chiavi di coppia, è necessario inviare la chiave PUBBLICA ai destinatari.

Con la chiave PUBBLICA i vostri destinatari possono criptare le e-mail che solo voi potete leggere.

Non inviate mai la vostra chiave PRIVATA

Per la crittografia, il destinatario deve importare la propria chiave PUBBLICA.

Importare il file ricevuto con la chiave PUBBLICA

Dopo l'importazione è necessario verificare questa chiave

Per la crittografia è necessario scegliere l'opzione Sicurezza e selezionare Richiedi crittografia.

Se tutto è a posto, il messaggio ricevuto è criptato.

Se si vuole crittografare i messaggi al destinatario, si deve importare la sua chiave pubblica.

Senza la chiave PRIVATA nessuno può vedere il contenuto dell'e-mail.

Non inviate mai la vostra chiave PRIVATA

Fare sempre una copia della chiave PRIVATA

Senza la chiave PRIVATA i vostri messaggi di posta elettronica saranno sempre cifrati e andranno persi

UNITÀ 3 - Settimana 5 - Sicurezza durante i viaggi di lavoro - VPN

VPN

In questo modulo imparerete a connettervi in modo sicuro alla rete informatica interna dell'azienda.

In questo esempio è stata utilizzata l'applicazione gratuita RADMIN VPN.

Si tratta di un sito web interno che può essere visualizzato solo nella rete aziendale.

Possiamo vedere che questo PC si trova nella rete interna.

Questo PC è collegato alla rete esterna e non è collegato alla rete aziendale.

Questo PC non riesce a collegarsi alla pagina web interna

Per creare questa possibilità è possibile utilizzare RADMIN VPN

Nel computer della rete interna scegliere Crea rete

Per la sicurezza inserire un nome di rete univoco e una password sicura

Nel PC remoto è sufficiente inserire il nome della rete e la password.

Ora è possibile provare a connettersi alla pagina web interna, ma prima è necessario verificare quale indirizzo IP ha

È possibile leggere il nuovo IP del server Enterprise VPN nell'applicazione RADMIN VPN.

Ora è possibile collegarsi alla rete interna

È inoltre possibile visualizzare le cartelle condivise nella rete interna.

Per interrompere questa connessione è sufficiente disabilitare Rete

Dopo aver disabilitato la connessione, non è possibile connettersi alla rete interna.

UNITÀ 3 - Settimana 5 - Sicurezza durante i viaggi di lavoro - Sicurezza delle reti wireless

Sicurezza della rete wireless

In questo modulo si apprenderà quale sicurezza di rete wireless è più sicura

Non è consigliabile connettersi alla rete wireless "aperta".

La vostra connessione può essere monitorata dagli hacker

Tentativo di connessione al tipo di rete più sicuro "WEP".

È bastata un'ora per violare qualsiasi password WEP.

Tentativo di connessione alla rete protetta di tipo "WPA2".

Sotto il nome della connessione WIFI si trova il tipo di connessione "Sicura".

Nell'impostazione il tipo di sicurezza wireless connessa è WPA2-Personale.

Gli hacker possono utilizzare il metodo della forza bruta per decifrare la vostra password

A questo scopo creano un dizionario con tutte le varianti dei caratteri.

Allora quanto tempo ci vorrà per decifrare la password?

Ci sono voluti circa 47 minuti per decifrare questa password

Allora come proteggere la rete wireless?

Utilizzate sempre password che:

- 1) Contengono almeno 9 caratteri
- 2) Contengono almeno un carattere maiuscolo e uno minuscolo.
- 3) Contengono almeno una cifra
- 4) Contengono almeno un carattere speciale come: "!"