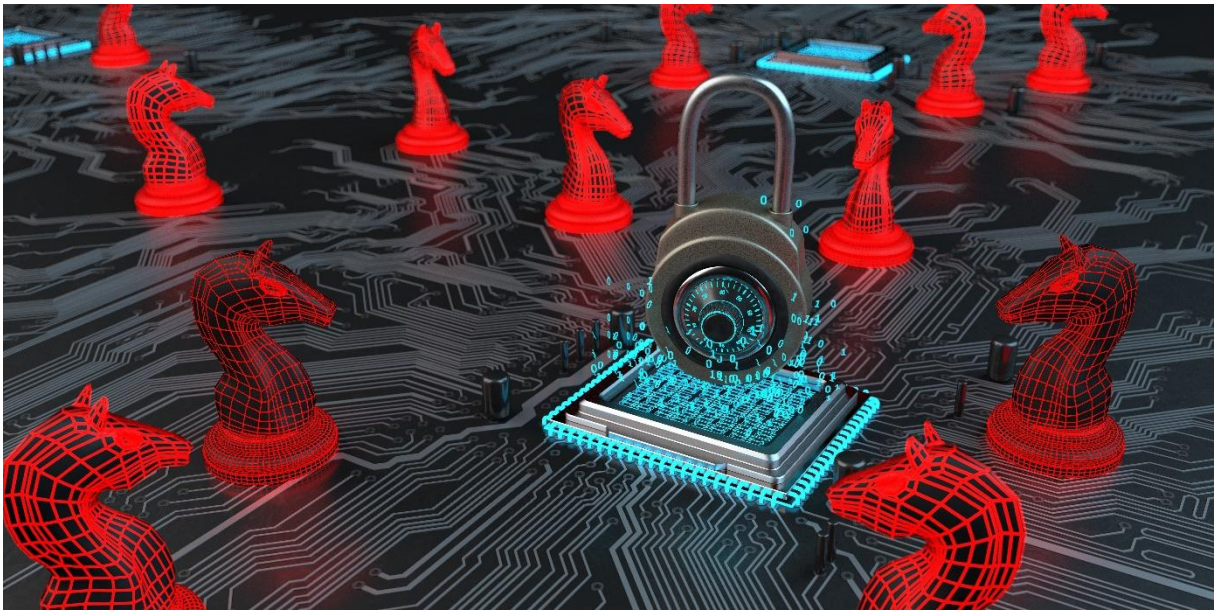
5. SICUREZZA INFORMATICA

5.1 Introduzione

La prima introduzione

Il backup dei dati era un tempo più semplice. In passato, documenti importanti come contratti o libretti di risparmio venivano generalmente rinchiusi in cassette di sicurezza o semplicemente nascosti. Ciò impediva alle persone non autorizzate di accedere o lo rendeva molto difficile.

Oggi non è più così semplice. Documenti e dati sono ora digitalizzati e spesso non sono più fisicamente disponibili. Pensa, ad esempio, al tuo banking online, a importanti contratti firmati elettronicamente e inviati tramite e-mail o dati privati come foto. Proprio come i documenti analogici erano "bloccati", al giorno d'oggi è necessario eseguire il backup digitale dei dati. Perché il potenziale furto di dati o l'elaborazione o la manipolazione illegale dei dati possono comportare rischi elevati e gravi conseguenze, sia per i privati che per intere società e organizzazioni..



La sicurezza IT, o "sicurezza delle informazioni", non è una novità, ma sta diventando sempre più importante a causa dei rapidi sviluppi digitali degli ultimi anni. E' necessario conoscerla, perché l'informazione digitale, che ne siamo consapevoli o no, è semplicemente la base della vita moderna.

La rilevanza pratica – per questo avrai bisogno delle conoscenze e delle abilità

Dalla vita privata al lavoro, dalle singole aziende alle corporazioni globali - i dati e le informazioni sono presenti in tutte le aree della vita e sono un bene prezioso. Che si tratti di criminalità informatica, perdita di dati, la sicurezza IT dovrebbe davvero interessare tutti. Questa unità di apprendimento ti aiuterà a garantire la sicurezza dei tuoi dati privati e a fornire un prezioso contributo alla sicurezza dei dati nella tua azienda. Sarai sensibilizzato sulla sicurezza IT in modo da acquisire dimistichezza con le questioni leate alla sicurezza informatica.

Obiettivi dell'apprendimento e competenze

In questo capitolo imparerai a conoscere il termine sicurezza IT nelle sue sfaccettature più importanti. Imparerai di più sul suo significato e obiettivi, ma anche su quali minacce e misure esistono attualmente nell'area della sicurezza IT. Imparerai a contribuire personalmente ad un ambiente informativo più sicuro, sia a livello privato che professionale.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Obiettivi dell'apprendimento
Conoscere e comprendere le definizioni generali e le aree di applicazione della sicurezza IT.
Essere in grado di nominare e spiegare gli obiettivi e le attività della sicurezza IT.
Conoscere le attuali minacce alla sicurezza informatica e assegnarle alla sicurezza IT nelle aree di applicazione.
Conoscere misure e meccanismi di difesa della sicurezza IT nell'applicazione

5.2 Definizioni e aree di applicazione

Quindi: la sicurezza IT non è solo sicurezza delle informazioni, sebbene spesso entrambi i termini siano usati allo stesso modo (specialmente se non tradotti esattamente dall'inglese in un'altra lingua), c'è una sottile differenza che ti aiuterà a definire il termine.

In linea di principio, questa differenza sta nella "T" del nome, perché la sicurezza IT sta per "Sicurezza informatica" o della Tecnologia dell'Informazione. Per praticità preferiamo l'espressione "sicurezza IT".

Definizione

Sicurezza delle informazioni vs. sicurezza IT

Il termine sicurezza delle informazioni indica misure di protezione per TUTTI i sistemi che elaborano o archiviano informazioni in qualsiasi modo. Non importa se sono digitali, un computer, o "analogici", una pila di documenti scritti a mano e riservati.

La sicurezza IT è una branca della sicurezza delle informazioni. In effetti, con questa espressione si intendono solo le misure di protezione dei cosiddetti sistemi "socio-tecnici". I sistemi socio-tecnici non sono altro che sistemi in cui gli umani usano la tecnologia dell'informazione per archiviare ed elaborare i dati.

Per inciso, secondo il dizionario, la tecnologia dell'informazione è definita come "tecnologia per la raccolta, la trasmissione, l'elaborazione e la memorizzazione di informazioni da parte di computer e apparecchiature di telecomunicazione".

Fin qui tutto bene. Tuttavia, poiché oggi solo in pochissime situazioni eccezionali non viene utilizzato affatto l'IT, la sicurezza IT copre gran parte della sicurezza delle informazioni.
Un esempio di mancato uso delle IT per la sicurezza delle informazioni potrebbe essere la ricetta segreta scritta a mano nella cassaforte del tuo ristorante preferito. Ma non è di questo che tratta questa unità.
Esistono anche altri concetti secondari nella sicurezza IT di cui è importante avere un quadro generale e comprendere come sono legati l'uno all'altro:

• **Sicurezza del computer**: si riferisce specificamente alle misure di sicurezza dei sistemi informatici locali e di rete stessi. Quanto è protetto un computer dall'accesso o dalla manipolazione non autorizzati? Cosa succede se un computer "si arresta in modo anomalo"?

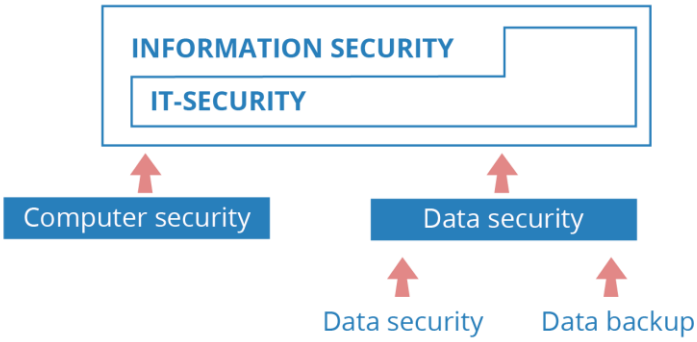
• **Protezione dei dati**: il termine è un vero è proprio trend, giustamente, perché "la protezione dei dati è protezione personale". Questo aspetto è particolarmente importante per il privato, perché riguarda la protezione dei propri dati personali dall'uso improprio. La privacy e l'anonimato sono una questione delicata in un mondo digitalizzato.

• **Sicurezza dei dati**: questo concetto è di natura più tecnica. Non si tratta tanto di questioni legali, ma semplicemente di come proteggere i dati da manipolazioni o perdite. La sicurezza dei dati può essere intesa come la fase tecnica preliminare per una protezione efficace dei dati.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

• **Backup dei dati**: si tratta in particolare di (multipli) backup dei dati - è molto probabile che abbiate familiarità con il termine "backup". E non è nient'altro che il backup dei dati: la corretta duplicazione dei dati per prevenirne la perdita.
Il diagramma seguente rende più chiaro il contesto di tutti i termini appresi:



La sicurezza IT costituisce gran parte della sicurezza delle informazioni e consiste principalmente nella sicurezza dei computer e dei dati. La sicurezza dei dati è la base per una protezione e un backup dei dati efficaci.

Importante
Dati e informazioni Hai letto i termini "dati" e "informazioni" così spesso, vorrai sicuramente conoscere la differenza: • I dati sono in realtà segni e simboli inutili - senza contesto, questi dati rimangono vuoti e non hanno nulla a che fare con esso. Prendiamo ad esempio la sequenza di numeri 19081974. • Le informazioni sono dati inseriti in un contesto. Questi dati diventano quindi significativi e trasmettono informazioni, ad esempio Data di nascita 08-19-1974 - è già chiaro cosa si intendesse per sequenza di numeri. A proposito, questa è anche l'idea alla base della crittografia, indipendentemente dal fatto che venga eseguita sul computer o manualmente. Lasci i dati senza contesto, forse potresti anche mescolarli. Solo qualcuno che comprende anche il contesto può comprendere il significato della sequenza di numeri.

Per chi è la sicurezza IT?
In realtà, per tutti coloro che hanno un computer, sia come individui che all'interno di un'organizzazione. In questo paragrafo classificheremo le aree di implementazione della sicurezza IT in modo un po 'più preciso, anche al fine di poter successivamente individuare per le minacce e le misure corrispondenti la corretta area di applicazione.
La principale distinzione da cui partire è tra uso privato o aziendale di dispositivi e dati.

Settore privato: riguarda individui e dispositivi utilizzati privatamente. Questo include il tuo laptop o smartphone, per esempio. Non importa se lo usi pubblicamente, ad esempio nella rete WLAN di un'università, l'importante è che tu lo utilizzi per gestire i tuoi dati privati.
Aziende e organizzazioni: si tratta di dispositivi che possono essere utilizzati per accedere ai dati di aziende o organizzazioni, ad esempio laptop o telefoni aziendali. Ciò si riferisce sia alle imprese commerciali sia alle società statali e alle organizzazioni, riguarda i dati condivisi, che appartengono a un'organizzazione.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Quali sono esattamente le differenze tra queste due aree di applicazione?

- **Area privata**

  Quasi ogni software presenta sempre errori di programmazione in un modo o nell'altro. Ciò può essere dovuto a inesattezze, ma anche semplicemente all'ignoranza, perché nessuno può sapere da quale "backdoor" o da quale caratteristica speciale nel codice del software si possa ottenere un accesso indesiderato.

  Ciò è particolarmente problematico perché la maggior parte dei dispositivi è costantemente connessa a Internet. Questi includono il computer privato, lo smartphone, lo smartwatch, ma anche la televisione o l'assistente vocale. Nella maggior parte dei casi, l'accesso "non autorizzato" o non autorizzato ai dati personali viene quindi effettuato via Internet. Il furto di dati può anche avvenire fisicamente, ad es. irrompendo e rubando il computer.
  Va notato: può accadere rapidamente, le password per l'online banking vengono rubate, i documenti importanti vengono persi o le foto private vengono rese pubbliche.

  La sicurezza IT è un argomento importante nel settore privato – sebbene sia limitata - sia per mancanza di consapevolezza da parte delle persone che utilizzano il sistema o anche per minori possibilità tecniche.

- **Aziende e organizzazioni**

  Quando si tratta di sicurezza IT nelle aziende, l'attenzione principale è ovviamente rivolta agli interessi economici. Sebbene l'implementazione tecnica della sicurezza IT sia di solito migliore rispetto al settore privato, la probabilità di essere vittime di attacchi IT è molto più elevata.

  Si pensi alle banche e alle compagnie assicurative che gestiscono molti soldi. O aziende all'avanguardia che vogliono proteggere i loro prototipi e idee dalla concorrenza.
  Anche qui i sistemi IT sono connessi via Internet. Un esempio di questo potrebbe essere l'uso di un servizio cloud da parte di diverse sedi aziendali: un server cloud fornisce spazio di archiviazione per i documenti che possono essere letti e modificati su Internet da tutte le posizioni. E' importante che solo le persone autorizzate possano accedere a questi documenti.

  Le grandi aziende hanno reparti che si occupano solo di sicurezza IT e investono molti soldi per rimanere aggiornati. Perché anche qui vale quanto segue: COME accadrà un attacco IT non è noto in anticipo, quindi la cosa principale è essere in grado di reagire rapidamente se si verifica un attacco.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

A proposito, esistono documenti standardizzati per la sicurezza IT, i cosiddetti cataloghi di protezione di base, che presentano modelli dettagliati di sicurezza IT. Tuttavia, l'IT si sta sviluppando così rapidamente che seguire questi cataloghi da soli non è sufficiente e alcuni di essi diventano rapidamente obsoleti.

Ricorda
La sicurezza IT è una branca della sicurezza delle informazioni e include tutte le misure di protezione nel trattamento e nella memorizzazione dei dati con l'aiuto dei sistemi informatici. Ciò include i computer e tutti gli altri mezzi di telecomunicazione in ambienti privati e aziendali. La sicurezza IT può essere suddivisa anche in sotto-aree collegate tra loro: • Sicurezza del computer • Protezione dati • Backup dei dati • La sicurezza dei dati La sicurezza IT riguarda sia la sfera privata che quella aziendale e pubblica. Poiché la maggior parte dei dispositivi è connessa a Internet, i pericoli degli attacchi IT e le misure per la sicurezza IT sono abbastanza simili in tutte le aree - le differenze si possono trovare nella consapevolezza personale e nei fattori tecnologici.

5.3 Obiettivi e funzioni della sicurezza IT

Il compito più importante della sicurezza IT è **seguire gli sviluppi tecnologici**. Il mondo della digitalizzazione e della rete sta progredendo molto rapidamente in termini di tecnologia. Le nuove tecnologie richiedono nuovi software, nuove aree di applicazione richiedono nuove misure di sicurezza.

Mentre in passato alcuni computer di grandi dimensioni svolgevano compiti per intere aziende e venivano gestiti da poche persone, oggi ci sono una miriade di piccoli dispositivi che sono tutti interconnessi.

Può essere abbastanza complicato anche spiegare cosa deve essere protetto esattamente da cosa, quali minacce ci sono e quali lacune nei sistemi di sicurezza potrebbero essere sfruttate.

Tuttavia, vengono definiti i cosiddetti obiettivi di protezione, ovvero gli obiettivi della sicurezza IT. Questi sono:

riservatezza - integrità - disponibilità

Se tieni a mente questi tre obiettivi di protezione, hai già implementato metà della sicurezza IT! Ecco come appaiono in dettaglio:

• **Riservatezza**
Dati, informazioni e conoscenze risultanti dovrebbero essere nascosti alle persone che non hanno il diritto di visualizzarli.

• **Integrità**
I dati, le informazioni e le conoscenze risultanti dovrebbero essere protetti da modifiche e manipolazioni non autorizzate.

• **Disponibilità**

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

I dati, le informazioni e le conoscenze risultanti dovrebbero essere accessibili a coloro che hanno consentito l'accesso, se necessario.
Questi tre obiettivi sono così importanti e centrali sia nel contesto privato che commerciale. Dai un'occhiata ai seguenti esempi:

Esempi
I tre obiettivi di protezione in un contesto privato usando l'esempio di "banking online" Si utilizza l'accesso online al proprio conto bancario. Questo è un problema delicato, perché sono in gioco i tuoi soldi. Come vengono raggiunti gli obiettivi di protezione qui? • Riservatezza: i dati di accesso, i dati dell'account e le password devono essere accessibili solo a te. • Integrità: nessuno dovrebbe poter effettuare trasferimenti online non autorizzati, tranne te. • Disponibilità: dovresti avere accesso illimitato al tuo account in qualsiasi momento e da qualsiasi luogo. **I tre obiettivi di protezione nel contesto aziendale utilizzando l'esempio di "sviluppo del prodotto"** Una società sviluppa un prodotto completamente nuovo che dovrebbe rivoluzionare il mercato. Naturalmente, ciò dovrebbe accadere senza che la concorrenza ne tragga profitto. Come potrebbero essere raggiunti gli obiettivi di protezione qui? • Riservatezza: tutte le informazioni sullo sviluppo del nuovo prodotto possono essere visualizzate solo da persone autorizzate. • Integrità: i dati ottenuti dallo sviluppo del prodotto sono protetti contro il sabotaggio e la manipolazione dall'esterno. • Disponibilità: tutte le persone coinvolte e autorizzate hanno accesso sicuro allo sviluppo del nuovo prodotto e ai dati risultanti.

Inoltre, ci sono anche obiettivi di protezione estesi che devono essere considerati in base ai requisiti. Questi non devono necessariamente essere ancorati alla sicurezza IT e possono variare notevolmente nel contesto privato e aziendale.

- **Responsabilità o anonimato**
  Un'azione nell'ambiente IT può essere chiaramente assegnata a una persona o no. Nel contesto aziendale, la persona responsabile del sabotaggio interno, ad esempio, può essere identificata. Nella vita privata, tra l'altro, è più probabile che accada il contrario, vale a dire che la persona gode del più grande anonimato possibile in relazione ai suoi dati - ad esempio, quando si effettuano ricerche su argomenti relativi alla salute su Internet.
- **Autenticità**
  Dati, informazioni e conoscenze risultanti dovrebbero essere verificabili per l'autenticità, ad esempio se i risultati della ricerca trasmessi sono originali o sono stati manipolati da terzi.
- **Non ripudio**
  Le azioni in un ambiente IT non devono essere negate: ciò è particolarmente importante per i contratti elaborati elettronicamente. Qui, ad esempio, vengono utilizzate le firme elettroniche.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Come si possono raggiungere concretamente questi obiettivi?

Questa domanda riguarda **i punti deboli**. O meglio, si tratta di trovare ed eliminare le vulnerabilità. Come hai già appreso, tutti i software presentano dei punti deboli. Questi non sono chiaramente identificabili come tali in anticipo. Spesso è dovuto alla scarsa programmazione del software utilizzato o alla progettazione del sistema IT. Ciò non significa necessariamente che sia stata fatta una programmazione "sbagliata", ma semplicemente che nella programmazione non sono state prese in considerazione tutte le minacce informatiche note. Tuttavia, i punti deboli possono anche essere l'essere umano o la gestione errata dei sistemi IT.

Importante
Naturalmente, la sicurezza IT può **anche bypassare tramite l'hardware** non solo tramite il software. Ma questo è più "poco pratico", perché per manipolare o rubare dati tramite l'hardware, devi essere fisicamente presente, ad esempio con una chiavetta USB in mano o rubando l'intero computer. Quindi, l'accesso al software via Internet è già più conveniente - e soprattutto più difficile da rintracciare se vieni sorpreso nel mezzo.

Al fine di raggiungere gli obiettivi di protezione della sicurezza IT, è quindi di enorme importanza identificare questi punti deboli e possibili scenari di minaccia. Ed è qui che diventa difficile, perché una rappresentazione al 100 percento di tutti i punti deboli non è affatto possibile a causa del costante sviluppo dei sistemi e dell'incapacità generale di guardare al futuro: si può solo approssimare il più vicino possibile.

Ricorda
La sicurezza IT **dipende fortemente dagli attuali sviluppi tecnologici**: nuove aree di applicazione della tecnologia dell'informazione comportano anche nuovi pericoli. Qui è necessaria una reazione rapida per essere in grado di offrire contromisure appropriate. Esistono **tre obiettivi di protezione** che devono essere raggiunti in tutte le aree di applicazione: • Riservatezza • Integrità • Disponibilità

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Esistono tre obiettivi di protezione aggiuntivi, che variano in base all'area di applicazione e devono essere considerati di conseguenza:

- Attribuibilità o anonimato
- Autenticità
- Impegno

Per raggiungere questi obiettivi di protezione **il compito principale della sicurezza IT è quello di identificare i punti deboli dei sistemi** e di eliminarli di conseguenza. Ciò può influire anche sull'hardware, ma attualmente piuttosto sul software: si riferisce principalmente a errori di programmazione o debolezze non considerate nella programmazione.

La perfetta sicurezza IT può essere approssimata, ma non soddisfatta al 100%. Ecco perché la sicurezza IT deve essere considerata nel suo insieme.

5.4 Minacce IT

Le minacce nell'IT sono molteplici e non devono necessariamente essere intenzionali o criminali. L'IT può anche essere minacciato da "forza maggiore" e / o guasti tecnici - ad esempio, un terremoto potrebbe causare un'interruzione di corrente con conseguente perdita di dati.

Ma ovviamente è anche concepibile un errore umano. Un classico esempio di questo è: la password per l'online banking è stata dimenticata, quindi le informazioni non sarebbero più disponibili.

Ora imparerai le possibili minacce IT: tieni sempre a mente gli obiettivi di protezione del capitolo precedente.

Importante
A proposito, una potenziale minaccia o vulnerabilità non significa automaticamente che l'IT è a rischio. Una minaccia effettiva è considerata una minaccia solo se una vulnerabilità (ad es. Errore di programmazione o WLAN facilmente accessibile) incontra una minaccia (ad es. Attacco di un hacker).

Attacchi mirati di persone o organizzazioni

Innanzitutto, naturalmente, sono gli attacchi che vengono deliberatamente eseguiti che devono essere evitati dalla sicurezza IT. Di solito indicato come "hacking", un individuo o persino un'intera organizzazione ottiene l'accesso non autorizzato a dati stranieri e cerca di aggirare gli obiettivi di protezione. Ciò può avere varie ragioni: furto di fondi, sabotaggio di aziende concorrenti, motivazione politica, a volte solo "divertimento" - ma si tratta sempre di ottenere, manipolare o distruggere informazioni straniere attraverso la rete a cui sono collegati i dispositivi di destinazione.

Gli strumenti più importanti di tali attacchi di hacking sono noti dai film di Hollywood del volgere del millennio e di solito hanno nomi divertenti: "virus", "trojan", "worm", "spoofing", "phishing" e altri. Diamo un'occhiata più da vicino ad alcuni di questi esempi:

- **Virus**
- I virus informatici sono semplicemente dei programmi che eseguono automaticamente le loro attività programmate nei sistemi di destinazione: ad esempio, per rintracciare una password. I virus hanno bisogno di un cosiddetto host per diffonderli. Può trattarsi di un'e-mail di massa o di un

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

cosiddetto "pop-up", ad esempio un sito Web ad apertura automatica che indica un presunto aggiornamento necessario.

- **Worms**
  Questi sono virus che possono diffondersi attivamente - ciò significa che rilevano attivamente i punti deboli nei sistemi e nelle reti e si inoltrano di conseguenza senza che sia presente un cosiddetto "host".

- **Trojans**
  Conosciuti anche come "cavalli di Troia", si tratta di programmi apparentemente utili che la vittima si installa da sé - ma sullo sfondo, i Trojan aprono in modo indipendente backdoor nel sistema, inoltrano dati e informazioni e possono, ad esempio, registrare le password inserite.

- **Attacchi Denial of Service**
  Qui, è più probabile che la disponibilità dei dati venga manipolata: sovraccaricando deliberatamente il sistema dall'esterno (ciò può essere fatto, ad esempio, richiamando automaticamente un sito Web in modo ripetuto), il sistema viene arrestato. A volte questo accade fino a quando l'organizzazione interessata paga un riscatto, per esempio. A proposito, il software per i metodi di ricatto viene anche chiamato "ransomware".

- **Spoofing/Phishing**
  Si tratta principalmente di furto di identità. I siti Web falsi su Internet e le e-mail che li collegano invitano la vittima a condividere attivamente password o informazioni sull'account. Questi si trovano principalmente nel settore privato della sicurezza IT.

- **Spam**
  A proposito, il termine probabilmente più noto in termini di sicurezza IT non descrive altro che e-mail indesiderate: possono essere fastidiose newsletter, ma ovviamente anche host di virus o tentativi di phishing.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Inviato: Lunedì, 9 Ottobre 2020

Da: ,,bmt.gv.at"

A: destinatario

Oggetto: notifica urgente per la sig.ra Muster

Fà attenzione:
- Indirizzo e-mail modificato
- E-mail spam
- Traduzione scorretta
- Oggetto e contenuto sospetto
- Link o allegato su cui cliccare

Cancella le email spam!

Gentile contribuente,

abbiamo identificato un errore nel calcolo della tassa dell'ultimo pagamento di €915,43.

Per restituire il pagamento. Abbiamo bisogno di alcuni dettagli per restituire la somma sul tuo conto in banca.

Compila il modulo allegato, e trasferiremo immediatamente la somma sul tuo conto.

Cordialmente,

Il Ministero federale delle Finanze

Naturalmente, il suddetto malware può anche essere "iniettato" personalmente nel sistema informatico: le informazioni possono essere rubate o manipolate irrompendo fisicamente nell'edificio o nella casa dell'azienda. A causa della rete di sistemi informatici, tuttavia, ciò non è più necessario.

Ma a volte tale manipolazione fisica avviene semplicemente internamente. Ad esempio, quando il personale dell'azienda ruba i dati dei clienti o i segreti dei prodotti senza autorizzazione per venderli esternamente.

Minaccia involontaria per errore umano

Ma le minacce alla sicurezza IT non devono sempre essere altamente criminali e intenzionali. A volte è semplicemente l'ignoranza nel trattare con l'IT che costituisce una minaccia:

- **Passwords**
  Una buona password è difficile da ricordare, ovviamente non è pratica. Molte persone usano ancora password troppo deboli. 12345 per esempio è una password debole. UfNS3-? SssDa-hUdk & - sembra abbastanza diverso - più simboli diversi, caratteri speciali, numeri e lettere, meglio è. Ma non se la password viene annotata di nuovo solo su un pezzo di carta direttamente sullo schermo.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Quindi vedi: trovare una password adatta e sicura che la persona interessata possa ricordare non è così facile. Soprattutto perché molti sistemi richiedono regolarmente di cambiare le password e non è consigliabile utilizzare la stessa password più di una volta.

Excursus

Esistono i cosiddetti **gestori di password** che possono essere utilizzati sia in privato che in azienda. Questi sono programmi che possono generare e archiviare password sicure per siti Web o programmi. Il programma stesso è protetto con una cosiddetta **chiave master**, ovvero UNA password principale.

I vantaggi e gli svantaggi sono evidenti: è possibile utilizzare una varietà di password diverse e sicure e non è necessario ricordarle singolarmente. Ma se la password principale è decifrata, è possibile accedere a tutte le password memorizzate. Un gestore di password è sicuro solo se la password principale è forte e preferibilmente modificata regolarmente.

Tuttavia, anche il passaggio di password è un problema. Questo non deve essere intenzionalmente negligente. Vuoi aiutare un collega e dargli rapidamente il tuo accesso al sistema. Oppure l'amministratore di sistema richiede la password per un controllo. Questo può portare a situazioni critiche, specialmente quando sono coinvolte persone che rubano deliberatamente le password in questo modo.

- **Portare il proprio dispositivo**

"Porta il tuo dispositivo" - questo non significa una festa di Natale selvaggia in compagnia, ma piuttosto prendere i tuoi dispositivi, come dischi rigidi esterni, chiavette USB, smartphone e simili. Se le informazioni interne all'azienda vengono archiviate o modificate su questi dispositivi, la sicurezza IT interna non può davvero aiutare. Ciò è particolarmente critico quando il cosiddetto "home office" è la pratica, vale a dire lavorare per un'organizzazione da casa.

A volte, a proposito, i supporti di archiviazione vengono deliberatamente "preparati" con malware da terze parti e quindi deliberatamente distribuiti a persone che lavorano per determinate aziende, ad esempio. Questo accade, ad esempio, in occasione di fiere professionali, in cui le chiavette USB vengono spesso regalate.

- **Installazione di applicazioni non autorizzate**

Il laptop aziendale è troppo lento, quindi "prenditi cura di te stesso" installando programmi antivirus e altre cose. Oppure ti piace giocare nel tempo libero al lavoro e scaricare malware sul tuo PC aziendale. Ciò può anche comportare minacce alla sicurezza IT a causa della mancanza di consapevolezza.

Queste sono essenzialmente le maggiori minacce alla sicurezza IT. Come già spiegato, eventi completamente imprevedibili possono ovviamente anche minacciare l'IT: disastri naturali come incendi, fulmini o inondazioni possono paralizzare o distruggere completamente i sistemi informatici.

Ricorda

Si parla di una reale minaccia in termini di sicurezza IT **quando una vulnerabilità interna incontra una minaccia esterna.**

Una tale minaccia può essere un attacco deliberato, non intenzionale da parte dell'uomo o di "forza maggiore" come un disastro naturale.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Attacchi deliberati:
- Malware come virus, worm e trojan
- Intrusione fisica e furto o manipolazione di informazioni o sistemi informatici
- Furto o estorsione di identità attraverso attacchi di phishing, ransomware e denial of action

Pericolo involontario
- Password deboli o trasmesse
- Utilizzo di dispositivi privati in ambienti aziendali
- Installazione di applicazioni non autorizzate

Forza maggiore
- Disastri naturali
- che successivamente portano alla distruzione o alla paralisi dei sistemi informatici

5.5 Misure di sicurezza IT

La sicurezza IT offre varie misure, non solo dal punto di vista tecnico. **Rendere le persone consapevoli di malware o comportamenti dannosi e inconsci nell'azienda o nelle loro vite private** di solito vale già molto.

A tal fine, vengono spesso offerti corsi di formazione e workshop, che possono prevenire uno dei problemi IT nella tua vita privata. All'interno delle aziende, a volte, intere strategie sono progettate per integrare la sicurezza IT in modo olistico e nel modo più completo possibile nei processi. Tuttavia, ciò non può funzionare senza prima sensibilizzare il personale.

Gli investimenti nell'informazione e nella sensibilizzazione non sono ovviamente sufficienti, quindi cos'altro fare per la sicurezza IT?

Software
Per prima cosa esiste un cosiddetto **software antivirus** che esegue automaticamente la scansione del sistema IT e verifica la presenza di malware. Ciò dovrebbe avvenire a intervalli brevi e regolari ed è utile sia in ambienti privati che aziendali. In questo modo è possibile rilevare e vietare lacune nel sistema di sicurezza e programmi dannosi scaricabili da Internet.

Lo sai già, ma non puoi ancora fare affidamento su di esso al 100 percento. A volte il malware non viene semplicemente rilevato come tale o il software sicuro viene identificato come malware, rimosso automaticamente e quindi il computer smette di funzionare. Pertanto, non è consigliabile fidarsi ciecamente di un programma antivirus.

I cosiddetti **firewall** sono anche mezzi popolari sia in contesti privati che aziendali. Si occupano delle connessioni di rete dell'IT, ad esempio con la WLAN. Qui è possibile rilevare e impedire l'accesso non autorizzato dall'esterno tramite la rete. Nella maggior parte dei casi, tali firewall sono già integrati nei prodotti software antivirus.

I **sandbox** sono qualcosa di particolarmente interessante, non solo per i bambini. Nella sicurezza IT, un sandbox sta per un programma che blocca il malware. Questo concetto relativamente nuovo è particolarmente efficace per tipi di dati speciali. Ad esempio, i documenti PDF vengono aperti in una "sandbox" separata dagli altri programmi. Se il PDF è danneggiato, nel peggiore dei casi viene attaccato solo il programma sandbox - il resto del sistema viene risparmiato.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

L'utilizzo di software diversi e talvolta la fiducia di provider più piccoli può ripagare, **più l'IT è "diversificata", più diventa difficile rompere il sistema nel suo insieme**. A volte le società di software antivirus più note sono particolarmente colpite dagli attacchi degli hacker, semplicemente perché sono le più comuni.

Controllo di accesso
Il controllo dell'accesso non significa semplicemente una password troppo lunga. Le aziende si aiutano con diritti utente diversi. **Solo pochissime persone nell'azienda hanno accesso a tutti i dati**, di solito questi sono limitati e divisi in base alla funzione dell'azienda.

È inoltre possibile implementare **l'accesso limitato alle pagine Internet** o la prevenzione di software esterni sui computer aziendali. La WLAN aziendale può anche essere progettata in modo tale da scaricare e utilizzare solo una selezione molto limitata di applicazioni e programmi.

Inoltre, esiste anche la possibilità di impedire il "contenuto attivo": i software auto-eseguiti (spesso si tratta di programmi di utilità) sono disattivati in questo modo. Questo può anche essere efficace contro potenziali malware. Le misure qui menzionate hanno ovviamente maggiori probabilità di essere applicate in un contesto aziendale.

Tuttavia, la **crittografia** può essere utilizzata per scopi aziendali e privati. Questo non significa altro che una crittografia dei dati. Non solo l'accesso ai dati è protetto con una password, ma i dati stessi sono anche "crittografati".

Excursus
Crittografia di dati e informazioni - end-to-end La crittografia end-to-end è uno standard comune nella crittografia dei dati. Qui mittente e destinatario hanno un codice traduttore. I messaggi o le immagini vengono inviati dal mittente. Tuttavia, il codice del traduttore modifica automaticamente i dati del messaggio in sequenze incomprensibili di numeri e simboli. Il destinatario li riceve e può a sua volta visualizzare e comprendere il messaggio o l'immagine nella sua forma originale grazie al traduttore**.** Questo serve semplicemente **affinché i dati eventualmente intercettati nel processo di invio non possano essere inseriti in un contesto** e quindi rimangono incomprensibili come informazioni.

Backup e Aggiornamenti

Naturalmente sono importanti anche gli aggiornamenti regolari del software. Più vecchio è un software, prima saranno noti i suoi errori. Soprattutto i sistemi operativi e i programmi antivirus dovrebbero essere prontamente aggiornati, poiché le maggiori minacce sono rappresentate dall'accesso esterno.

Naturalmente, c'è solo una cosa che può aiutare contro la perdita di dati (se, ad esempio, il computer viene rotto o rubato): backup regolari, cioè la copia di dati e informazioni da soli - preferibilmente tenuti separati dal sistema IT su un disco rigido esterno o nel cosiddetto "cloud". I sistemi cloud sono server esterni e posizioni di archiviazione disponibili via Internet. Qui, un backup può anche essere automatizzato, ma ovviamente c'è anche il rischio che il provider cloud stesso diventi vittima di un attacco IT.

Ricorda
Rendere le persone consapevoli della corretta gestione della sicurezza IT, sia in ambito privato che aziendale, vale già molto.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Esistono anche diverse misure di sicurezza IT:

Software

- Programmi antivirus
- firewall
- sandbox
- Diverso uso del sistema IT

Controllo di accesso

- Diritti utente diversi
- Accesso limitato a siti Web e programmi su Internet
- Crittografia

Misure aggiuntive

- Backup regolari
- Ultimi aggiornamenti

5.6 Riassunto

La sicurezza IT è una branca della sicurezza delle informazioni e indica tutte le misure di protezione nel trattamento e nella memorizzazione dei dati in un sistema IT, sia nel settore privato che in quello aziendale. Ciò include **sicurezza del computer, protezione dei dati, backup dei dati e sicurezza dei dati.**

La sicurezza IT dipende fortemente dagli **attuali sviluppi tecnologici**. Soprattutto, è necessario reagire rapidamente per poter offrire contromisure appropriate. Vi sono **tre obiettivi fondamentali di protezione** che devono essere raggiunti in tutte le aree operative:

riservatezza - integrità - disponibilità

Al fine di raggiungere questi obiettivi di protezione, **il compito principale della sicurezza IT è identificare i punti deboli nei sistemi ed eliminarli di conseguenza.** Una vera minaccia nel senso di sicurezza IT è quando una vulnerabilità interna incontra una minaccia esterna.

Tale minaccia può essere **un attacco deliberato** a fine di rubare o manipolare dati (ad esempio con malware su Internet o irrompendo fisicamente nel dipartimento IT di un'azienda).

Ma un sistema IT può anche essere **minacciato involontariamente**, ad esempio, da una password debole o da catastrofi naturali in cui i sistemi informatici sono danneggiati.

Rendere le persone consapevoli della corretta gestione della sicurezza IT, sia privatamente che nelle aziende, può già aiutare. Inoltre, sono disponibili **software di protezione, controlli di accesso restrittivi** e altre misure di sicurezza IT per ridurre al minimo le potenziali minacce.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.