Profilo Nemici

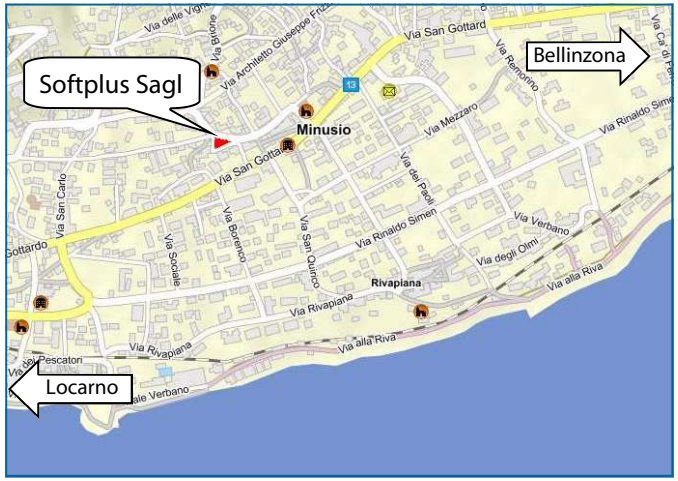
- **Hackers** - professionisti della pirateria informatica che prendono possesso di accessi aziendali per danneggiare dati o farne uso ponte per altri attacchi
- **Insider** - ex collaboratori o collaboratrici scontenti o inefficienti che asportano dati dall'azienda o li danneggiano o fanno un uso improprio di internet
- **Esploratori** - clienti, colleghi, conoscenti, visitatori che per curiosità trafugano dati o informazioni d'accesso

Attacchi

- **Virus** - sono i più pericolosi. Si propagano sulla rete e cancellano file e inibiscono l'uso dei sistemi
- **Trojans** - mascherati da software spesso scaricati dalla rete sono veicoli per distribuire codice distruttivo o inviare e-mail con copie di propri file
- **Attacchi di ricognizione** - vengono utilizzati per raccogliere informazioni e testare il sistema si sicurezza della rete al fine di architettare un attacco. Ottenuto con software come sniffer, scanner o programmi di decifrazione password

Danni ed effetti

- **Danni economici** - il danno economico può derivare da molteplici effetti dell'attacco: distruzione o evasione di informazioni riservate, interruzione di servizio e perdita di business, spese legali derivanti da danni generati a terzi, necessità di bonifica del sistema e rafforzamento delle misure di sicurezza, ecc.
- **Danni legali** - causati da rivalsa di terzi per danni concatenati all'attacco subito, rivalsa di terzi per violazione della privacy su dati personali persi o danneggiati
- **Danni d'immagine** - per servizi erogati a terzi e resi inaffidabili da attacchi portati con successo, senso di fragilità trasmesso da un sistema che non garantisce adeguata sicurezza, invio improprio di mail o dati riservati a terzi



softplus
Data Base Giannini

Softplus Sagl

Via Brione 15
Casella postale 1253
6648 Minusio

091 730 1111
www.softplus.ch

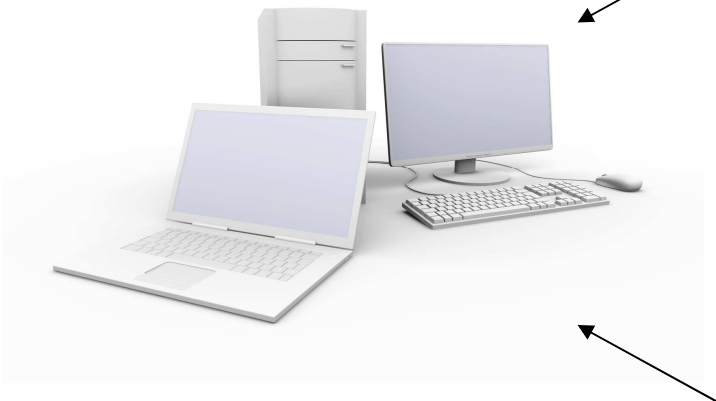
swisscom
Partner

La sicurezza dei vostri dati

Dalla perdita improvvisa o dall'accesso non autorizzato alle vostre informazioni

La sicurezza dei vostri dati

Perdita dati improvvisa
La perdita improvvisa di una parte o di tutti i dati aziendali e/o privati mette l'utente di fronte ad un problema che molto spesso non viene preso in considerazione fintanto che non accade, mettendo in grave crisi la produttività dell'azienda. Le cause più frequenti di questi eventi sono le rotture dell'hardware, virus, furto, incendio e imperizie da parte dell'utente.
Per questo motivo è molto importante che una solida soluzione di backup possa garantire il recupero dei propri dati nel più breve tempo possibile per tornare produttivi.



Rotture harddisk
Virus
Incendio / Incidente
Imperizia utente

Soluzione

Virus / Spyware
Trojans / Phishing
Furto
Accessi non autorizzati

Soluzione

Accesso non autorizzato ai vostri dati
I pericoli di accesso ai vostri dati da persone non autorizzate sono molteplici. Ex collaboratori scontenti, conoscenti e visitatori possono essere tra questi. Ma altrettanto l'intromissione di hackers, facilitati da sistemi non aggiornati o da software malevolo presente nel PC, come virus, spyware e trojans.
In questi casi, le conseguenze legate ai danni subiti, oltre all'aspetto produttivo, possono essere rivalse legali da parte di terzi per danni concatenati all'attacco o per violazione della privacy su dati personali persi o danneggiati, così pure come un'immagine negativa dell'azienda qualora la notizia dell'intromissione è resa pubblica.

Backup (copie di sicurezza)

- Analisi del sistema di backup adottato
- Ottimizzazione o creazione di una soluzione di backup in base alle esigenze dell'utente e del tipo di infrastruttura informatica (non solo dei dati ma dell'intero sistema operativo)
- Verifica dei tempi e funzione di ripristino
- Costante controllo tramite notifiche giornaliere del sistema di backup (email, logs, ecc.)

1. Analisi della sicurezza dell'infrastruttura

- Focalizzare quali sono i servizi aperti verso l'esterno (mail server, web, VPN, ecc.)
- Verifica dei routers e apparecchi di rete
- Analisi del server: logs di sistema, controllo stato aggiornamenti
- Verifica dei criteri di sicurezza password

2. Intervento

- Configurazione apparecchi di rete: politica restrittiva (Firewall, NAT)
- Rimozione servizi non necessari su server e ottimizzazione in base alle problematiche dei logs
- Impostazione "strong password" e breve panoramica sui criteri di sicurezza password agli utenti

3. Verifica

- Scansione dall'esterno delle porte e dei servizi attivi
- Controllo complessità password d'accesso utenti