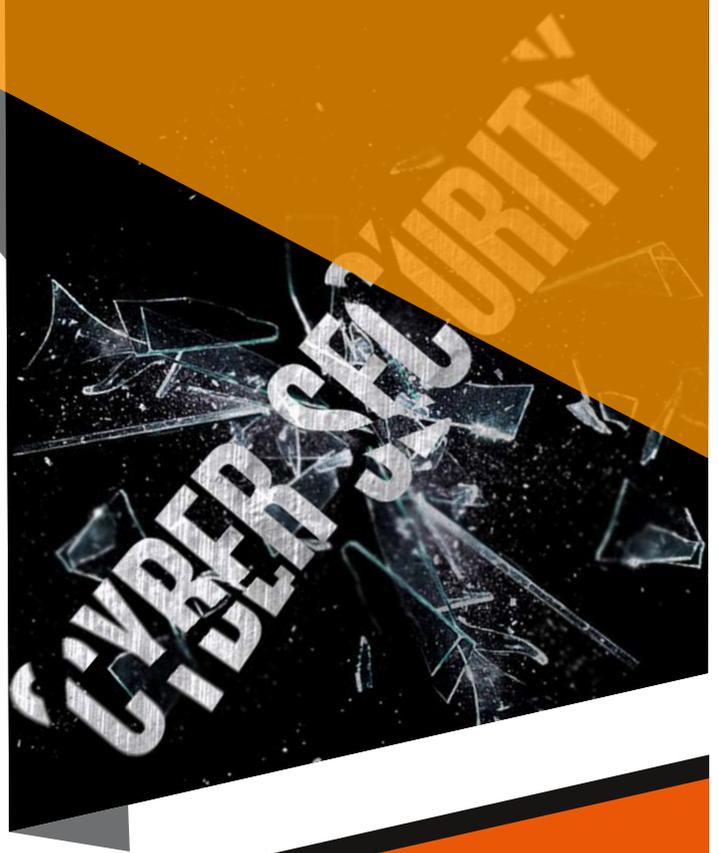


## Un sistema ICT sicuro

Personalizzazione della configurazione della rete e dei sistemi

### Come proteggere la rete

- ❖ Configurare il router in modo appropriato (filtri antispoofing, filtri che consentono l'accesso solo ai servizi istituzionali).
- ❖ Segmentare la rete in sottoreti separate, applicando, in relazione al contesto, le politiche più rigorose:
  - Sottorete DMZ esposta a Internet (DNS, server Web, server di posta)
  - Sottorete per Management e Amministrazione
  - Sottorete per didattica e laboratori
  - Sottorete per studenti e ospiti (BYOD: smartphone, tablet, notebook)
  - Sottorete per stampanti, videosorveglianza, automazione degli edifici, dispositivi IoT, ecc.
- ❖ Installare almeno un firewall di rete che blocchi le connessioni in entrata a tutte le sottoreti (esclusa DMZ), eventualmente anche con la funzione di NAT.
- ❖ Attenuare gli attacchi effettuati tramite e-mail analizzando i messaggi prima che raggiungano la casella del destinatario. A tale scopo, configura il software antispam e antivirus sul server di posta.
- ❖ Installa una soluzione di filtraggio web per proteggere gli utenti da siti dannosi durante la navigazione.
- ❖ Abilitare la sicurezza wireless:
  - Utilizzare il più potente protocollo di crittografia disponibile (WPA2/WPA3)
  - Cambiare la password predefinita di amministratore del router
  - Modificare il Service Set Identifier (SSID) predefinito
  - Disabilitare il WiFi Protected Setup (WPS)
  - Ridurre la potenza del segnale wireless
  - Spegnerne la rete quando non in uso (o configurare un'accensione programmata della rete wireless)
  - Disabilitare l'Universal Plug and Play (UPnP)
  - Mantenere tutti i router e i dispositivi di rete aggiornati all'ultima versione del firmware
  - Disabilitare la gestione remota
  - Monitorare i tentativi di connessione di dispositivi sconosciuti.



### Firewall

I firewall forniscono protezione contro gli aggressori esterni preservando i computer o la rete da traffico di rete malevolo o non necessario.

I firewall possono anche impedire al software dannoso di accedere ai computer o a una rete tramite Internet.

I firewall possono essere configurati in modo da bloccare i dati da determinati indirizzi di rete, applicazioni o porte consentendo al tempo stesso l'accesso ai dati rilevanti e necessari.

I firewall richiedono professionisti qualificati per supportare la loro configurazione e manutenzione. La maggior parte dei prodotti firewall viene preconfigurata ed è pronta per l'uso. Poiché ciascun firewall è diverso, è necessario leggere e comprendere la documentazione fornita per determinare se le impostazioni del firewall predefinito sono sufficienti per le proprie esigenze.

I firewall non garantiscono che il tuo computer non venga attaccato.

I firewall aiutano principalmente a proteggere dal traffico dannoso, non dai programmi dannosi (ad es. malware) e potrebbero non proteggerti se accidentalmente installi o esegui malware sul computer. Tuttavia, l'utilizzo di un firewall insieme ad altre misure protettive (ad es. software antivirus e pratiche informatiche sicure) rafforzerà la resistenza agli attacchi.





## Come proteggere i sistemi

Definire e implementare le configurazioni standard e le politiche di protezione dei sistemi:

- ❖ Disinstallare software non necessari
- ❖ Disabilitare i servizi non necessari
- ❖ Condividere solo le risorse hardware necessarie e proteggerle
- ❖ Impedire le modifiche alla configurazione o l'installazione del software da parte di utenti non amministratori
- ❖ Impostare correttamente le configurazioni software e hardware predefinite (molti prodotti hanno una configurazione predefinita troppo aperta)
- ❖ Configurare client e server per utilizzare solo protocolli crittografati: SSH, HTTPS, IMAP e SMTP su SSL/TLS
- ❖ Installare localmente il software antivirus (e verificarne l'aggiornamento automatico)
- ❖ Installare localmente firewall e sistema di prevenzione delle intrusioni (IPS)
- ❖ Installare un Web Application Firewall (WAF) sul server Web
- ❖ Disabilitare l'esecuzione automatica dei contenuti quando si collegano dispositivi rimovibili
- ❖ Disabilitare l'esecuzione automatica di contenuti dinamici (ad esempio macro) nei file
- ❖ Disattivare l'apertura automatica delle e-mail
- ❖ Disabilitare l'anteprima automatica del contenuto del file
- ❖ Prima di connettere un nuovo dispositivo alla rete, sostituire le credenziali amministrative predefinite



The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 - Up2U