

Guida pratica alla sicurezza ICT per il progetto Up2U

L'ecosistema Up2U si basa sull'uso di Internet, dei sistemi cloud e sull'approccio Bring Your Own Device (BYOD). La creazione di un ambiente di apprendimento ICT sicuro e protetto per tutte le scuole coinvolte nei progetti pilota è una delle nostre priorità. Questa guida offre consigli pratici e semplici alle scuole su come ottenere tale ambiente.

Consapevolezza, responsabilità e procedure per tutta la scuola 9 consigli per insegnanti e amministratori di sistema

Istituire una Task Force per la sicurezza

Nella Task Force sulla sicurezza suggeriamo di inserire tutte le risorse umane che, all'interno della scuola, possano aiutare a identificare i rischi e creare una visione comune sulla sicurezza ICT. La collaborazione completa ad ogni livello è fondamentale.

Gestire tutti gli utenti

- ❖ Per i sistemi che gestiscono informazioni riservate, si consiglia di applicare rigide configurazioni utente. Per poter associare gli utenti ai dispositivi e contattarli in caso di necessità, è indispensabile creare un registro degli utenti.
- ❖ Usare gli account standard con privilegi limitati. Consentire l'uso di account amministrativi solo per gli utenti con competenze appropriate.
- ❖ Usare gli account amministrativi solo per eseguire operazioni che richiedono determinati privilegi.

Creare un inventario hardware e software

- ❖ Si consiglia di creare un inventario (in maniera manuale o con software automatico) dei dispositivi esistenti collegati alla rete, registrando il MAC address, l'host name, la funzione, il proprietario, l'ufficio associato, ecc.
- ❖ Potrebbe essere utile un sistema di allarme che, in caso di anomalie, rilevi i dispositivi connessi in rete e identifichi i dispositivi elettronici portatili.
- ❖ Creare un elenco del software autorizzato e un inventario del software installato.
- ❖ Effettuare scansioni regolari del sistema per rilevare software non autorizzati.



Creare una policy per la sicurezza

Una policy per la sicurezza scolastica deve affrontare, come minimo, quanto segue:

Rendere chiaro agli utenti che:

- Le risorse IT vanno utilizzate solo per scopi istituzionali
- Devono evitare di usare videogames e scaricare software illegali (MP3, film, ecc.)
- È vietato lanciare attacchi informatici su sistemi interni ed esterni

Informare regolarmente gli utenti sulle precauzioni:

- Fare attenzione alle e-mail di phishing. Alcuni indizi per individuarle sono:
 - ◆ Forte carattere di urgenza
 - ◆ Indirizzo del mittente sospetto
 - ◆ Saluti generici e firma altrettanto generica
 - ◆ Collegamenti ipertestuali contraffatti
 - ◆ Ortografia e layout (grammatica scadente)
 - ◆ Allegati sospetti
- Evitare di navigare su siti non affidabili e di cliccare su link sospetti
- Scaricare e installare software e app solo da siti affidabili
- Eliminare programmi o app non più utilizzati

Migliorare la sicurezza delle password:

- Assicurarsi che gli utenti:
 - ◆ Non rivelino mai le password, specialmente via Internet;
 - ◆ Rendano le password lunghe e complesse (almeno 12 caratteri, mescolando lettere maiuscole, numeri e simboli). È possibile creare una password lunga utilizzando una passphrase, vale a dire quattro o più parole casuali raggruppate e utilizzate come password;
 - ◆ Creino una password univoca per ogni account.
 - ◆ Non usino mai le informazioni personali come password;
 - ◆ Prendano in considerazione l'utilizzo di un gestore di password.
- Forzare periodicamente la modifica della password
- Utilizzare l'autenticazione a due fattori, se disponibile

Tenersi aggiornati!

- ◆ Mantenere aggiornato tutto il software (applicazioni e sistema), in modalità automatica se consentito.
- ◆ Tenere aggiornati anche tutti i dispositivi elettronici personali. I produttori rilasciano gli aggiornamenti man mano che scoprono vulnerabilità nei loro prodotti. Gli aggiornamenti automatici lo rendono più semplice per molti dispositivi, inclusi computer, telefoni, tablet, ma per altri dispositivi potrebbe essere necessario l'aggiornamento manuale. Installare gli aggiornamenti dai siti web dei produttori e dagli archivi di applicazioni incorporati: i siti e le applicazioni di terze parti non sono affidabili e possono infettare i dispositivi. Quando si acquistano nuovi dispositivi, valutare il mantenimento del produttore per garantire regolari aggiornamenti di supporto.
- ◆ È importante restare aggiornati sulle nuove vulnerabilità e intraprendere azioni di manutenzione regolari.
- ◆ Utilizzare strumenti di scansione delle vulnerabilità aggiornati.
- ◆ Verificare che le vulnerabilità emergenti dalle scansioni siano state risolte mediante patch o implementando contromisure appropriate o documentando e accettando un rischio ragionevole.
- ◆ Utilizzare solo software e sistemi operativi supportati (ad esempio, evitare Windows XP).
- ◆ Il vettore di attacco principale è il browser, soprattutto se non è aggiornato!

Sii consapevole!

- ◆ Controllare i log delle operazioni del server DHCP (generalmente abilitato per impostazione predefinita).
- ◆ Gestire ogni accesso alla rete registrando l'account, il timestamp, il MAC address e l'indirizzo IP.
- ◆ Eseguire periodicamente una valutazione della vulnerabilità interna e esterna per identificare preventivamente le proprie vulnerabilità prima che lo faccia qualche malintenzionato.

Implementare un programma di backup

- ◆ Eseguire backup regolari di dati critici e, a intervalli più lunghi, dell'intero sistema. Ci sono molte soluzioni cloud che possono aiutarti a farlo.
- ◆ Garantire la riservatezza dei dati nelle copie di backup mediante crittografia. La crittografia eseguita prima della trasmissione consente un backup remoto sicuro nel cloud.
- ◆ Assicurarsi che i dispositivi rimovibili contenenti backup (ad esempio, dischi rigidi esterni o pen drive USB) non siano accessibili in modo permanente dal sistema, per evitare che gli attacchi locali coinvolgano anche le copie di sicurezza.



- ◆ Attenzione all'inserimento di dispositivi USB sconosciuti nei sistemi scolastici. Potrebbero contenere un malware nascosto!
- ◆ Una policy affidabile di backup dei dati può salvarti se sei colpito da ransomware.

Creare una procedura per la gestione degli incidenti

Ogni scuola dovrebbe avere un piano di risposta agli incidenti informatici. Se le persone sanno cosa fare in caso di problemi, il loro impatto può essere ridotto al minimo.

Dopo l'incidente, dovresti documentare ciò che è successo e condividere tutte le informazioni, per prevenire casi simili in futuro.

Adottare le Acceptable Use Policy

Ogni utente della rete deve firmare una Acceptable Use Policy per la sicurezza ICT.

Le scuole possono rifarsi ai modelli e alle linee guida presenti sul sito web della rete WMnet (www.wmnet.org.uk).