GDPR SCUOLA
LO STAFF TECNICO DEL DIRIGENTE

Guida al lavoro sicuro a scuola e da casa

Giacomo Lunardon

Servizi Tecnici Istituto Statale “A. Monti” di Asti e “CIS Controls Volunteer”

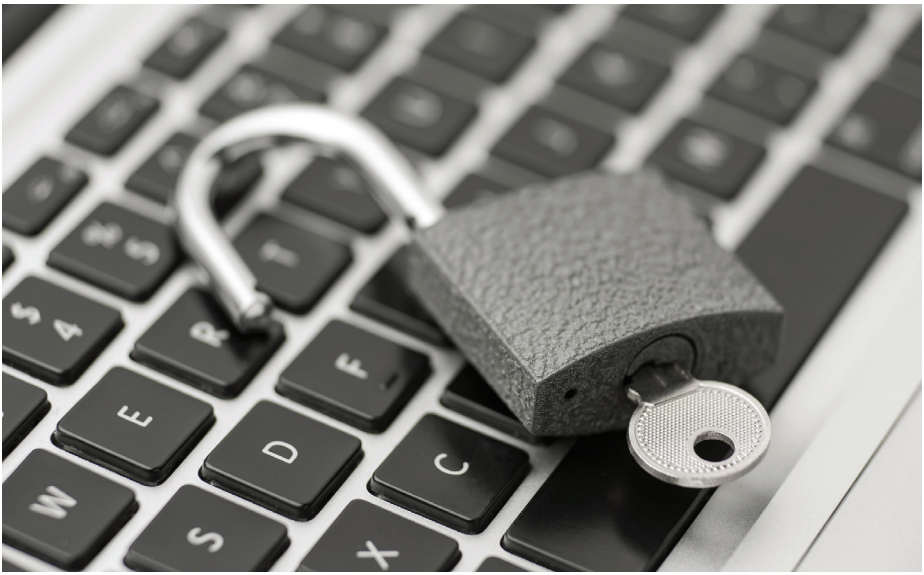
L'importanza di lavorare in sicurezza

Quanto è importante per un docente o per chi lavora in segreteria a scuola operare in massima sicurezza, onde evitare di compromettere l'integrità dei dati trattati?

Gli episodi di cybercrime sono in costante aumento negli ultimi anni, e non risparmiano il settore dell'istruzione, pesantemente colpito da attacchi ai danni dei server che contengono le informazioni personali degli utenti della scuola.

Ma come fare allora a difendersi dagli hacker?

In questo piccolo manuale vediamo quali sono le principali procedure da seguire per limitare il rischio informatico dei dispositivi di rete, elementi fondamentali per la comunicazione tra computer.



I dispositivi

Router, modem e altri dispositivi sono gli strumenti che consentono la connettività a internet.

Sebbene siano sviluppati e commercializzati per uso domestico, vengono spesso acquistati da organizzazioni di piccole e medie dimensioni e utilizzati per il lavoro quotidiano.

In genere non si sa come siano configurati o protetti, e per questo bisognerebbe considerarne il livello di sofisticazione tecnologica, fatto non trascurabile in caso di minaccia volta allo spionaggio dei dati di navigazione, delle password, ecc.

Fortunatamente le impostazioni di sicurezza possono essere configurate per rafforzare in modo significativo queste difese.

Considerazioni generali

Le considerazioni sulla sicurezza informatica riferibili all'uso di dispositivi di rete si possono riassumere secondo i seguenti punti:

- Se qualcuno accede fraudolentemente alla rete può leggere dati sensibili come informazioni fiscali, identificazione personale, e altri elementi che non devono essere condivisi con altri
- La compromissione di un router può comportare l'inserimento in una "botnet", che può essere usata per attaccare altri sistemi informatici e organizzazioni
- Il mancato rispetto delle basilari procedure di sicurezza informatica può configurarsi in qualche modo come responsabilità per violazioni e perdite di dati causati da computer non sicuri

- In caso di adozione di un'assicurazione per la sicurezza informatica, la compagnia assicurativa richiederà al titolare dell'infrastruttura IT di applicare adeguate misure di sicurezza

Acquisto di un dispositivo di rete

Con poche eccezioni, una volta acquistato un router o un altro dispositivo di rete, generalmente non è possibile applicare ulteriori funzionalità di sicurezza.

Ciò significa che lo strumento più adatto alle nostre esigenze deve essere cercato e verificato prima di comprarlo.

Per maggiore chiarezza si riportano alcuni termini comuni utilizzati (spesso in modo intercambiabile) per indicare questi dispositivi.

Prima di procedere con l'acquisto, si consiglia in ogni caso di chiedere chiarimenti al rivenditore, e di leggere bene quali sono le caratteristiche del dispositivo sul sito della casa produttrice.

Modem

Un modem comunica con la rete di un provider di servizi Internet (ISP), ed è il dispositivo principale necessario per l'accesso alla rete.

È spesso fornito dall'ISP, anche se nel tempo può essere più economico acquistarne e gestirne uno da soli.

Possono essere indicati anche come decoder via cavo o "modem digitali" per il collegamento alla linea (DSL).

Questi apparati sono ad esempio le "chiavette internet", collegabili al PC utilizzando la porta USB.

Router

Un router è un dispositivo che gestisce tipicamente una rete interna, agendo come "hub".

In un ambiente piccolo i router si collegano direttamente al modem tramite un cavo ethernet fisico.

Un altro dispositivo simile, chiamato "switch di rete", può essere utilizzato per creare connessioni ethernet aggiuntive, ma non dispone delle funzionalità del router.

I router moderni generalmente fungono anche da punto di accesso wireless (WAP), agendo anche da firewall, e gestiscono gli indirizzi IP tramite il protocollo DHCP.

Modem e router ibridi

In passato router e modem erano dispositivi distinti, ma attualmente i moderni acquisti (oppure i dispositivi forniti dall'ISP) integrano entrambe le funzionalità, e sono conosciuti anche come "gateway".

Estensore

Il termine identifica un apparato in grado ampliare il raggio d'azione di una rete WI-FI e utilizzato nelle aree in cui il segnale wireless è debole o assente per ampliare l'area di copertura.

Questo metodo per estendere il segnale offre una serie di vantaggi sia per gli utenti che per il proprietario del dispositivo, come ad esempio la creazione di una rete wireless separata o la riduzione del numero di WAP.

Possono essere forniti e dall'ISP o acquistati separatamente in un negozio di elettronica, e sono conosciuti anche come "estensori WI-FI" o "estensori di portata".

Amplificatori di segnale cellulare

I ripetitori di segnale cellulare funzionano in modo simile agli estensori WI-FI, rendendo più facile l'accesso alla rete cellulare.

Questi dispositivi sono necessari quando la copertura non è presente o non è sufficiente all'interno di un edificio, e sono conosciuti anche come "estensori cellulari" o "gateway cellulari".

Caratteristiche di sicurezza minime

Il mercato dei router è abbastanza competitivo, e spesso vengono aggiunte nuove funzionalità per aiutare i dispositivi a distinguersi dalla massa.

Se si decide per un acquisto, vale la pena considerare i seguenti elementi:

- Frequenza degli aggiornamenti software: questa funzione garantisce che gli aggiornamenti di sicurezza siano regolarmente forniti dal produttore
- Aggiornamento automatico: questa funzione garantisce che gli aggiornamenti di sicurezza forniti dal produttore siano installati con regolarità sul dispositivo
- WPA3: la Wireless Protected Access versione 3 (WPA3) è l'ultima versione del WI-FI standard, e contiene protocolli di autenticazione e crittografia più evoluti
- Rete ospite: le reti ospiti possono fungere da linea di separazione tra dispositivi affidabili e dispositivi non attendibili, e forniscono anche un modo per offrire l'accesso alla rete ad altri utenti senza comunicare la password della rete WI-FI principale
- Firewall integrato: un firewall blocca o consente il traffico di rete secondo le esigenze
- Rete privata virtuale (VPN): una VPN riserva un canale di comunicazione tra due punti remoti connessi a internet in modo sicuro e riservato
- Controllo genitori: l'obiettivo di questa funzionalità è quello di impedire l'accesso a siti con contenuti non autorizzati, illegali o pericolosi per la sicurezza della rete
- Autenticazione a due fattori (2FA): ulteriore meccanismo attivabile per consentire o negare l'accesso ad altri dispositivi o risorse di rete

Dove acquistare apparecchiature di rete

L'elemento più importante da tenere in considerazione è l'affidabilità della fonte.

L'acquisto di un dispositivo usato è rischioso, sia per motivi di sicurezza in termini di password e account, sia per la non sicura disponibilità di supporto tecnico o garanzia in caso di guasto.

Setup del dispositivo

Dopo aver rimosso il dispositivo dalla confezione, è bene - se possibile - registrarsi sul sito del produttore, in modo che la garanzia venga attivata correttamente per eventuali problemi tecnici futuri.

È anche opportuno conservare qualsiasi supporto fisico (DVD, CD, USB) e le credenziali fornite con il dispositivo in un luogo sicuro: potrebbero essere utili per ripristinare le impostazioni di fabbrica o per effettuare operazioni amministrative particolari.

Si tenga conto inoltre di conoscere bene la procedura per aggiungere, modificare o disabilitare gli account amministrativi e cambiare le password.

Bisogna altresì assicurarsi di disabilitare le reti WI-FI preimpostate eventualmente presenti nel dispositivo.

Accesso iniziale

Il manuale utente del dispositivo illustra il metodo per accedere al portale amministrativo dove si possono modificare le impostazioni di configurazione.

Comunemente l'accesso avviene attraverso un'applicazione web integrata, per mezzo di un programma dedicato, o tramite browser (in questo caso puntando a un indirizzo specifico come 192.168.1.1 o 192.168.0.1).

Sebbene non sia obbligatorio, è più sicuro eseguire le operazioni amministrative con una connessione cablata, adottando preferibilmente protocolli sicuri, come ad esempio HTTPS.

Interfacce di rete interne e esterne

Router e modem sono dotati di varie schede di rete per consentirne la funzionalità agendo da gateway tra la rete domestica e il fornitore del servizio internet.

A prescindere, bisogna sempre essere consapevoli del tipo di accesso fornito da un router, controllandone il traffico tramite un firewall per gestire in modo opportuno le connessioni in entrata e in uscita.

Password

Le password sono una parte delle credenziali principali utilizzate per accedere al dispositivo tramite il processo noto come "autenticazione".

Tutte le password devono essere ragionevolmente forti e lunghe almeno otto caratteri o più.

La password amministrativa va inoltre sempre cambiata, rimpiazzando le impostazioni predefinite di fabbrica.

Deve poi essere univoca, e non condivisa se non con persone di fiducia o incaricati professionalmente preparati.

Tipi diversi di password utilizzate per i dispositivi di rete includono:

- Password rete WI-FI: utilizzata per accedere alla rete wireless, e che sarà probabilmente condivisa con altri
- Password amministrativa del router: utilizzata per accedere alla dashboard di configurazione, o correlata all'applicazione specifica utilizzata per la gestione
- Password ISP: utilizzata per accedere al portale online dell'ISP

Attenzione! Molti router sono configurati con password predefinite. Tali password sono facilmente disponibili online, rendendone estremamente facile l'individuazione.

Applicazioni per la gestione dei dispositivi di rete

Alcuni produttori di router forniscono anche app di gestione della rete per funzioni amministrative utilizzabili sugli smartphone.

Queste app consentono di usare una password per accedere al router, ma un'opzione possibile è quella dell'utilizzo di un'autenticazione 2FA, che è significativamente più sicura.

Se si usa un dispositivo mobile per eseguire attività di manutenzione, esso deve avere gli ultimi aggiornamenti software installati e configurati correttamente.

Setup della rete

Una volta che un nuovo dispositivo di rete è collegato a una fonte di alimentazione, è probabile che si avvii e inizi a trasmettere in automatico a una o più reti WI-FI.

In caso di due wireless, il dispositivo compare spesso con lo stesso nome, o SSID (Service Set IDentifier), e le due connessioni sono distinguibili solo per la frequenza operativa.

Ad esempio, i nomi di rete a 5 Gigahertz (GHz) spesso assomigliano a "NomeRete-5Ghz".

Questo perché il WI-FI funziona a due frequenze diverse (2,4 GHz e 5 GHz), e ogni rete può essere trasmessa separatamente sulle due lunghezze d'onda.

Naturalmente, una volta ottenute le credenziali di accesso, entrambe le reti possono essere modificate e gestite secondo necessità.

Posizionamento del dispositivo

La posizione fisica di un dispositivo di rete fa una grande differenza in termini di sicurezza.

I dispositivi devono essere tenuti in un'area lontana dal pubblico, in quanto l'accesso fisico al router spesso comporta il rischio che qualcuno entri nella rete senza una password WI-FI.

Inoltre, non tutte le interfacce interne potrebbero supportare il cambio di password, e per questo una corretta collocazione del router è fondamentale.

Nome della rete WI-FI

Dare un nome a una rete può essere un'attività divertente, ma può anche aiutare a individuare una persona o un'attività lavorativa.

Questo può diventare un problema per il telelavoro, e si devono adottare quindi alcune semplici misure come:

- Pensare in anticipo se una rete debba individuare o meno un individuo, una attività, un ufficio specifico
- Valutare se sia necessario includere informazioni sulla dislocazione fisica (ad esempio "UfficioContabile" oppure "Interno14")
- Considerare se serva oppure no trasmettere il nome della rete, oppure mantenerla nascosta

Creare una rete "guest"

Le reti ospiti sono utili perché separano i dispositivi con dati sensibili da altri che potrebbero non essere affidabili.

Dove possibile si possono adottare due router separati, oppure attivare la funzione di rete ospite, se prevista dal dispositivo.

È comunque fondamentale condividere la password di rete WI-FI con il minor numero possibile di persone.

Utilizzando due router separati, ciascuno con una propria password e connessione indipendente, si possono facilmente separare i dispositivi affidabili e quelli non affidabili.

Il lato negativo di questa configurazione è costo di gestione.

Talvolta sono anche disponibili funzionalità della rete ospite con password temporanee e specifiche restrizioni d'uso in termini di orari e quantità di dati utilizzati.

Abilitare gli aggiornamenti automatici

Gli aggiornamenti software sono estremamente importanti per proteggere qualsiasi dispositivo di rete.

Vengono costantemente scoperti nuovi difetti di sicurezza e vulnerabilità, e il modo principale per difendersi da questi problemi è l'installazione degli aggiornamenti.

Sfortunatamente alcuni produttori non li rilasciano in modo costante, e pertanto è opportuno acquistare un prodotto di comprovata esperienza nella fornitura degli "update".

Anche se è accettabile approvare e installare manualmente gli aggiornamenti, per esigenze di telelavoro sarebbe meglio attivarli in modalità automatica.

Criptare il traffico di rete

La crittografia è una tecnica che permette di trasformare i dati e impedire che le informazioni trasmesse vengano lette o modificate da chi non è autorizzato.

Esistono molti tipi di crittografia, alcuni più potenti ed altri meno efficaci, e per questo obsoleti.

Garantire il giusto tipo di crittografia impedirà ad altri di visualizzare dati sensibili, informazioni, ecc. senza che ne abbiano l'autorizzazione.

Di seguito sono riportati protocolli e chiarimenti correlati alla crittografia e all'autenticazione.

WEP (Wired Equivalent Privacy)

È stato il primo metodo di crittografia integrato in punti di accesso wireless per WI-FI.

Fu introdotto per la prima volta alla fine degli anni '90, ma è considerato insicuro, e non dovrebbe essere utilizzato.

Viene principalmente conservato nei dispositivi per motivi di compatibilità, ma la tecnica di crittografia è facilmente violabile utilizzando un software gratuito e disponibile su web

WPA (WI-FI Protected Access)

Questa tecnologia è stata introdotta per sostituire il precedente sistema WEP, ed è anche conosciuta come WPA-Personal o WPAPSK.

Sebbene WPA sia una tecnologia piuttosto sicura, non è completamente inattaccabile per chi ha una specializzazione, conoscenze e attrezzature.

Il suggerimento è quello di abbandonare la tecnologia WPA quando i sistemi WPA2 e WPA3 sono disponibili.

WPA 2 (WI-FI Protected Access Version 2)

WPA2 è lo standard per le reti di tutto il mondo.

La crittografia è affidabile e utilizza lo standard Advanced Encryption Standard (AES).

Esistono vari tipi di WPA2, alcuni pensati per l'uso aziendale, che sono più difficili da configurare.

Una delle principali differenze tra WPA2-Personal e WPA2-Enterprise è il metodo di distribuzione della password.

In linea di massima WPA2-Personal è sufficiente per le esigenze di piccoli uffici e home office.

WPA 3 (WI-FI Protected Access Version 3)

WPA3 è la più recente forma di sicurezza wireless per WI-FI, ed è attualmente in fase di implementazione in nuovi dispositivi in tutto il mondo.

I principali vantaggi in termini di sicurezza di WPA3 includono le chiavi di dimensioni maggiori e una più sicura procedura di autenticazione iniziale.

La problematica futura potrebbe essere legata alla necessità di sostituire i device meno recenti che non supportano tale funzionalità.

WPS (WI-FI Protected Setup)

WPS consente la facile connessione WI-FI, generalmente premendo un pulsante situato sul router stesso.

Il sistema è stato progettato per semplificare la connessione degli utenti, ma sfortunatamente sono state rilevate diverse vulnerabilità abbastanza facili da sfruttare, che possono consentire agli aggressori di connettersi alla rete WI-FI senza autorizzazione.

Se possibile, questa tecnologia dovrebbe essere disabilitata.

Ulteriori configurazioni di rete

I router e altre apparecchiature di rete possono essere ulteriormente configurati in vari modi.

Il funzionamento varia a seconda dei produttori, ma le seguenti opzioni sono presenti nella maggior parte dei dispositivi.

Firewall

I firewall aiutano a prevenire un danno, controllando le informazioni che entrano in una rete per raggiungere determinati dispositivi.

Sono generalmente integrati nella maggior parte dei router, ma la loro utilità ed efficacia talvolta può essere difficile da comprendere.

Un router con un firewall integrato potrebbe essere più costoso, ma come regola generale le strutture con reti più grandi e complesse o con servizi di connessione a internet dovrebbero prendere in considerazione l'acquisto di un modello dotato di questa tecnologia.

La maggior parte delle funzionalità può essere impostata su più livelli (tipo "sicurezza bassa", "sicurezza media" e "sicurezza alta"), anche se si suggerisce sempre di utilizzare le impostazioni più rigorose disponibili durante la configurazione iniziale.

Se queste impostazioni non consentono agli utenti di accedere ad alcune risorse web, si può ridurne la sicurezza per soddisfare le esigenze del piccolo ufficio o dell'home office.

La maggior parte dei router integra il Network Address Translation (NAT), che funziona nascondendo dispositivi e reti situati dietro al router, rendendo la struttura più difficile da attaccare.

L'utilizzo di NAT è talvolta indicato come "mascheramento IP", e deve comunque essere sempre abilitato.

"Hardening" dei dispositivi

Gran parte della protezione avanzata dei dispositivi consiste nella rimozione di porte e servizi attivi generalmente non utilizzati.

I servizi possono essere pensati come "programmi" che hanno lo scopo di comunicare con sistemi informatici esterni.

Le porte possono essere immaginate come passaggi verso l'esterno, e sono identificate da un numero e/o da un protocollo (UDP 53, TCP 80).

In genere ogni servizio utilizza una porta dedicata per comunicare: rimuovere i servizi in esecuzione e chiudere le porte accresce il livello di protezione dei dispositivi collegati alla rete.

DNS (Domain Name System)

Il DNS è un metodo per associare gli indirizzi IP ai nomi dei siti web.

In sostanza, ogni volta che un computer nella rete interna richiede una pagina web, un server DNS è utilizzato per cercare dove si trova la pagina stessa su internet.

Una rete domestica e relativi dispositivi collegati utilizzano generalmente un server DNS pre-configurato, e nella maggior parte dei casi fornito dal service provider.

Esistono opzioni DNS alternative, e alcune organizzazioni offrono server dedicati che possono aiutare a impedire che i sistemi informatici raggiungano siti web pericolosi.

L'utilizzo del filtro DNS permette quindi un blocco preventivo in caso si tenti di raggiungere un indirizzo o URL pericoloso.

Tra questi DNS citiamo quelli più noti, come Quad 9 (www.quad9.net) e OpenDNS (www.opendns.com).

Le organizzazioni possono scegliere la configurazione individuale più opportuna per ogni computer workstation, tablet o dispositivo mobile, oppure configurare il router per proteggere l'intera rete.

Per i dispositivi che vengono utilizzati al di fuori del luogo di lavoro si consiglia la prima soluzione.

UPnP (Universal Plug and Play)

È una suite di protocolli di rete che consente ai dispositivi di comunicare facilmente, spesso utilizzata per condividere dati tra computer, stampanti e periferiche di gioco senza necessità di configurazione.

Purtroppo negli anni si sono riscontrati problemi di sicurezza per questo tipo di protocolli, e per questo dovrebbero sempre essere disabilitati.

Se UPnP è assolutamente necessario per il funzionamento di un'organizzazione bisogna utilizzare solo la versione più aggiornata, anche se questo non può essere facilmente verificabile dell'acquisto del dispositivo.

Nella maggior parte dei casi devono essere disponibili funzioni di configurazione manuali, utili per impostare modalità operative alternative a UPnP.

MAC (Media Access Control) nella "whitelist"

La whitelist degli indirizzi MAC può essere utilizzata per impedire ai dispositivi di accedere a un WI-FI o a una rete cablata.

Gli indirizzi MAC sono come i numeri di serie per qualsiasi dispositivo dotato di cavo o connessione senza fili.

L'inserimento di indirizzi MAC nella whitelist richiede l'aggiunta manuale di ogni indirizzo MAC riferito a ogni dispositivo tramite l'apposita interfaccia di gestione del router.

Sfortunatamente gli indirizzi MAC possono essere facilmente falsificati, portando a un falso senso di sicurezza, che può essere aggravato dalla difficoltà di gestione del router.

Un malintenzionato, se dotato di capacità e software adeguato, può tenere traccia degli indirizzi di tutti dispositivi connessi a una rete, anche se crittografata, e con pochi comandi clonare qualsiasi MAC utile per accedere a una rete WI-FI in modo fraudolento.

Considerando la grande quantità di lavoro necessaria per mantenere la whitelist degli indirizzi MAC e la scarsa efficacia della protezione fornita, non se ne consiglia l'utilizzo.

Sicurezza di rete - La "check list"

La seguente lista di controllo contiene le azioni che dovrebbero essere messe in atto dopo aver acquistato un dispositivo di rete.

A seconda del prodotto, è possibile che alcuni degli elementi riportati non siano applicabili al caso specifico.

Si presentano comunque due procedure, una "semplificata", ed una invece "evoluta", la quale prevede tuttavia il possesso di capacità e tecnologie di livello professionale per essere implementata.

Questa ulteriore "check list" potrà essere applicata per una situazione di infrastruttura più ampia e complessa.

Check list semplificata

- Registrare il dispositivo sul sito del produttore e conservare una copia del feedback di registrazione
- Modificare la password amministrativa predefinita di tutti i router e i modem, adottandone una univoca per ciascun dispositivo
- Utilizzare una password unica per accedere al portale web del proprio ISP (Internet Service Provider)
- Abilitare l'autenticazione a due fattori, ove possibile
- Cambiare il nome della rete WI-FI (SSID), adottando termini o sigle univoci
- Assicurare che il nome della rete WI-FI (SSID) fornisca informazioni di identificazione indispensabili
- Prestare attenzione a chi vengono distribuite le password della rete WI-FI
- Disattivare la rete 2,4 GHz o 5 GHz se una delle due non viene utilizzata

- Spostare tutti i router e i modem in un luogo non accessibile al pubblico o a persone in genere non autorizzate
- Abilitare gli aggiornamenti automatici per tutti i router e i modem
- Attivare WPA2 o WPA3
- Disattivare WPS, se possibile
- Abilitare il firewall del router e/o del modem
- Abilitare il filtro DNS sul router e/o sul modem
- Disabilitare UPnP

Check list "evoluta"

- Mantenere un inventario dei punti di accesso WI-FI
- Effettuare una scansione delle vulnerabilità della rete, e ricercare inoltre l'eventuale presenza di punti di accesso WI-FI non autorizzati
- Disabilitare l'accesso wireless su dispositivi che non hanno necessità lavorative per la connettività WI-FI
- Configurare l'accesso WI-FI sui client che hanno una reale necessità, e consentire l'accesso solo alle reti autorizzate, limitando nel contempo l'accesso ad altre reti
- Disabilitare sui dispositivi connessi alla rete WI-FI le funzionalità di connessione ad altri dispositivi per mezzo di bluetooth e NFC

GDPR SCUOLA

LO STAFF TECNICO DEL DIRIGENTE

Vuoi ricevere un supporto qualificato e costante nel tempo per affrontare i problemi relativi a privacy e GDPR?

Richiedi informazioni

Telefono: 0163 03 50 22

Email: team@gdprscuola.it

www.gdprscuola.it