

TAGLIANDO SICUREZZA

Le procedure indispensabili a salvaguardare
la protezione della tua azienda da rischi
e attacchi informatici.



Tagliando Sicurezza Monitoro

Con l'aumento esponenziale di attacchi capaci di sfruttare le vulnerabilità di programmi e apparati presenti all'interno delle infrastrutture informatiche aziendali, è aumentata anche la frequenza con cui vengono rilasciate patch di sicurezza e aggiornamenti e da parte delle case produttrici.

Diventa pertanto di fondamentale mantenere tutte le componenti software e hardware costantemente allineate alle ultime release disponibili.

Esigenza di fronte alla quale Monitoro ha risposto introducendo il **Tagliando Sicurezza**. Una sequenza dettagliata di interventi tecnici al fine di **preservare e certificare il grado di sicurezza dell'intera rete informatica aziendale**.

Perché gli aggiornamenti sono importanti?

Anche se un software sembra funzionare normalmente, non significa che lo stesso non presenti lacune o problemi nascosti. Periodicamente le case produttrici rilasciano patch e aggiornamenti per risolvere i cosiddetti "bug", delle "falle" da colmare per renderne più sicuro e performante l'utilizzo.

Per un hacker ogni bug rappresenta un piccolo spiraglio da poter tramutare in un accesso diretto all'intera rete informatica interessata.

Pertanto, qualsiasi mancato aggiornamento rappresenta una vera e propria falla di sicurezza dell'infrastruttura.

Le tre MacroFasi

Il Progetto Tagliando Sicurezza coinvolgerà sia la Divisione Sistemistica che la Divisione Web. Per ogni categoria strumentale, è prevista una procedura operativa standardizzata i cui esiti saranno parte integrante della relazione a certifica di fine lavoro.

FASE 1

Preanalisi



In questa prima fase il nostro team operativo si occuperà di identificare le appliance e i sistemi inclusi nell'infrastruttura per cui è necessario e consigliato effettuare un aggiornamento.

FASE 2

Organizzazione e Intervento



Un referente Monitoro incaricato stenderà una pianificazione dettagliata della sequenza dei processi e degli eventuali fermi da imporre ai servizi in uso da sottoporre ad approvazione del cliente prima dell'esecuzione effettiva degli interventi.

FASE 3

Report e Certificazione



Il lavoro si conclude con la stesura di un report dettagliato. Una vera e propria attestazione certificata dello svolgimento e dell'esito delle prime due fasi del Tagliando Sicurezza.

FASE 1

Preanalisi

In virtù del grado di aggiornamento dei diversi dispositivi e software presenti in azienda, vengono identificate ed effettuate le seguenti operazioni.



Applicazioni

Installazione di patch e aggiornamenti cumulativi di software di servizio come Microsoft Exchange, Microsoft SQL, Apache, Php, Wordpress, Joomla, Mysql, Applicazioni Custom e Siti Web gestiti o realizzati direttamente da Monitoro.



Server

Aggiornamento di Sistemi Operativi Microsoft Server e Linux, di virtualizzatori Vmware ESXI/vSphere e di firmware/drivers della casa produttrice del device.



Client (PC)

Aggiornamenti di sistemi operativi Microsoft Windows 10, Microsoft Office, drivers/aggiornamenti della casa produttrice del dispositivo.



Dispositivi

Installazione di drivers e firmware rilasciati dalla casa produttrice del dispositivo quali firewall, switch, stampanti e printserver.



Wifi

Aggiornamento all'ultima release di software e drivers rilasciati dalla casa produttrice del dispositivo quali access point, antenne e apparati concentratori.



Autenticazione

Come imposto dal GDPR, configurazione della pianificazione periodica del cambio password degli utenti che accedono agli applicativi.



Backup

Verifica del rilascio aggiornamenti da parte della casa produttrice del servizio o software di backup e conseguente installazione.

FASE 2

Intervento

Aggiornare un sistema o un apparato senza creare un disservizio a utenti e operatori dello stesso, non è sempre possibile. Per questo motivo, nell'ottica di una migliore organizzazione operativa, **la pianificazione di modalità e tempistiche di intervento verrà pre-concordata con il cliente.**

Non tutte le operazioni incluse nel Tagliando Sicurezza implicheranno un intervento in loco. Infine, è bene ricordare che ogni sistema o apparato può prevedere tempistiche di aggiornabilità differenti in virtù di più fattori:



Status Aggiornamento

Apparati o sistemi non aggiornati da tempo possono implicare più passaggi intermedi.



Riavii Previsti

Il riavvio può non essere unico, perciò non sempre il tempo necessario è prevedibile.



Prestazioni Internet

Una connessione poco performante può rallentare il download degli aggiornamenti.



Livello di Criticità

Alcuni interventi necessitano di un backup preventivo e successiva verifica al riavvio.

“

L'obiettivo di **Monitoro** è ridurre quanto più possibile disagi o fermi di lavoro consentendo allo stesso tempo al suo team di **concludere il Tagliando Sicurezza in tempi certi e modi celeri.**

FASE 3

Report Interventi e Certificazione

A conclusione del piano operativo, al cliente verrà consegnata una relazione redatta dal team tecnico coinvolto.

Il Report conterrà:



Elenco delle fasi previste



Interventi eseguiti



Esito delle operazioni

La sua funzione sarà quella di certificare gli esiti di tutte le operazioni effettuate e il relativo grado di sicurezza ottenuto.



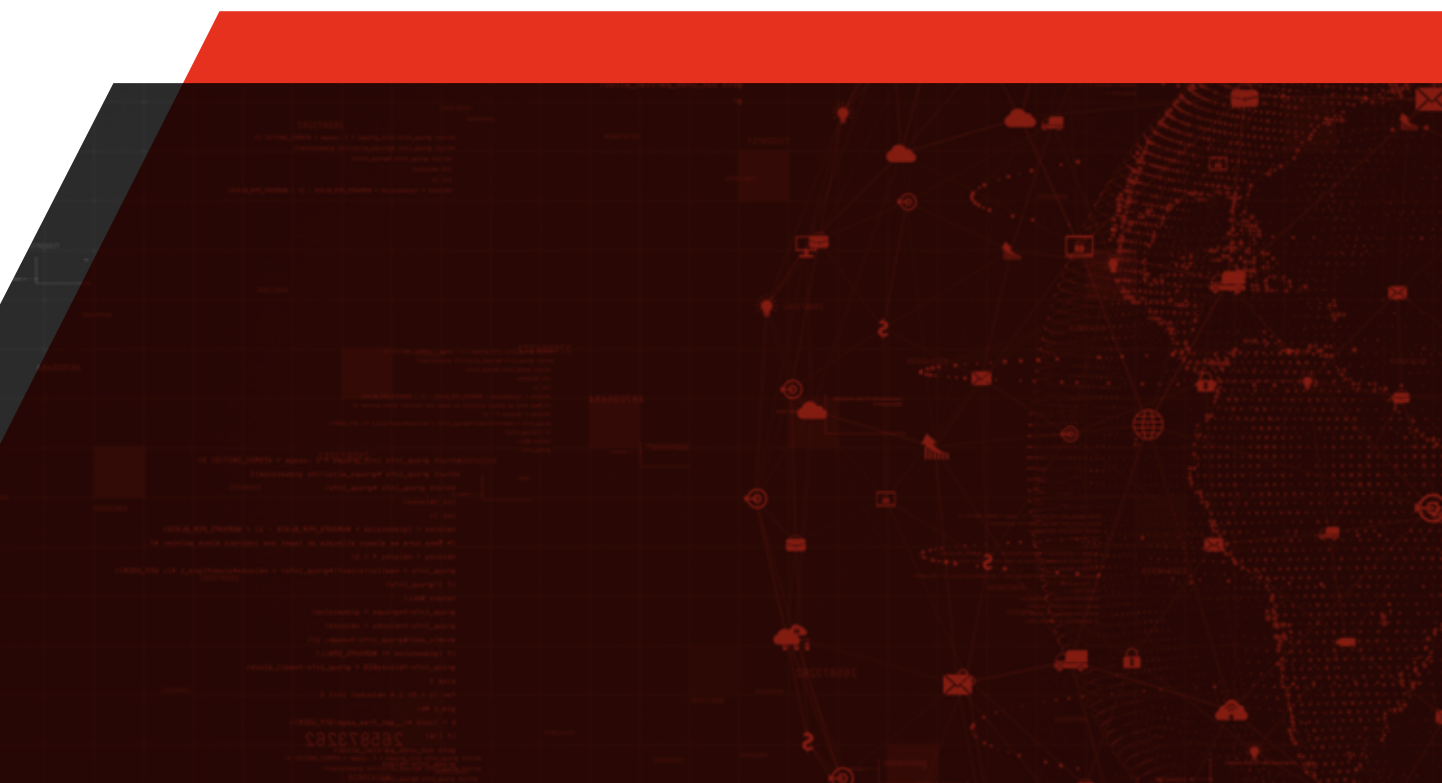
MONITORAGGIO

Il punto di forza del Tagliando Sicurezza

L'impatto in termini di tempo e risorse per effettuare il primo Tagliando Sicurezza è senza dubbio di una certa importanza. Per questa ragione, diventa opportuno monitorare con frequenza il grado di aggiornabilità ed il livello di vulnerabilità degli strumenti sui quali è stato eseguito l'intervento.

A tale scopo, durante l'esecuzione della FASE 2, **saranno introdotti degli AGENT DI MONITORAGGIO su tutti i sistemi ed i dispositivi trattati.**

Tali installazioni consentiranno al nostro team di verificare con costanza l'eventuale necessità di aggiornamento e/o le vulnerabilità di ciascun componente hardware o software. Così facendo, sarà possibile **mantenere nel tempo il grado di sicurezza e di performance dell'intera infrastruttura informatica aziendale** raggiunto con il primo Tagliando Sicurezza.



TAGLIANDO SICUREZZA

Il Progetto Monitoro ideato per preservare e certificare il grado di sicurezza e protezione della tua infrastruttura informatica aziendale.

Via Cremona, 10 (EuroPalace Piano 2)
25025 Manerbio (BS)
Tel. 030 777 8487 - Fax 030 777 3304
info@monitoro.it - monitoro@pec.it
commerciale@monitoro.it

www.monitoro.it

