

SPECIALE

GARANTIRE LA SICUREZZA DELLE INFRASTRUTTURE CRITICHE

Nel corso degli anni i sistemi di controllo industriale sono diventati più aperti verso il mondo esterno ed è cresciuta la loro vulnerabilità agli attacchi dalla rete. In uno scenario in cui cyber crime e terrorismo sono sempre più vicini, preoccuparsi della sicurezza delle infrastrutture critiche diventa quanto mai importante. **pag. 7-17**



CYBER ATTACK

PONEMON: 4 MILIONI DI DOLLARI IL COSTO DI UN INCIDENTE DI CYBER SECURITY

Aumentano i costi medi delle violazioni alla sicurezza dei dati secondo lo studio annuale del Ponemon Institute, sponsorizzato da IBM: più precisamente la crescita è del 29% rispetto al 2013, che porta il costo medio di un "cyber security incident" a 4 milioni di dollari. **pag. 3-6**

PROTAGONISTI

GASTONE NENCINI, TREND MICRO: DIFENDERSI DAL FURTO DEI DATI

Le informazioni sono la vera fonte vitale di ogni azienda. I metodi per sottrarre i dati aziendali diventano sempre più sofisticati, sfuggenti ed efficienti nei risultati. Trend Micro, grazie a un ventaglio di soluzioni integrate e tecnologie distintive, abilita una protezione a 360 gradi. **pag. 19**



IN QUESTO NUMERO:

CIBER ATTACK

pag. 3

Costa 4 milioni di dollari un incidente di cyber security

SPECIALE

pag. 7

Garantire la sicurezza delle infrastrutture critiche

pag. 11

Kaspersky Lab e la sicurezza dei sistemi industriali

pag. 12

Le linee guida per la sicurezza delle infrastrutture critiche

pag. 14

L'unione fa la sicurezza

pag. 16

Acea Distribuzione più sicuro con le soluzioni di Check Point

SOLUZIONI

pag. 19

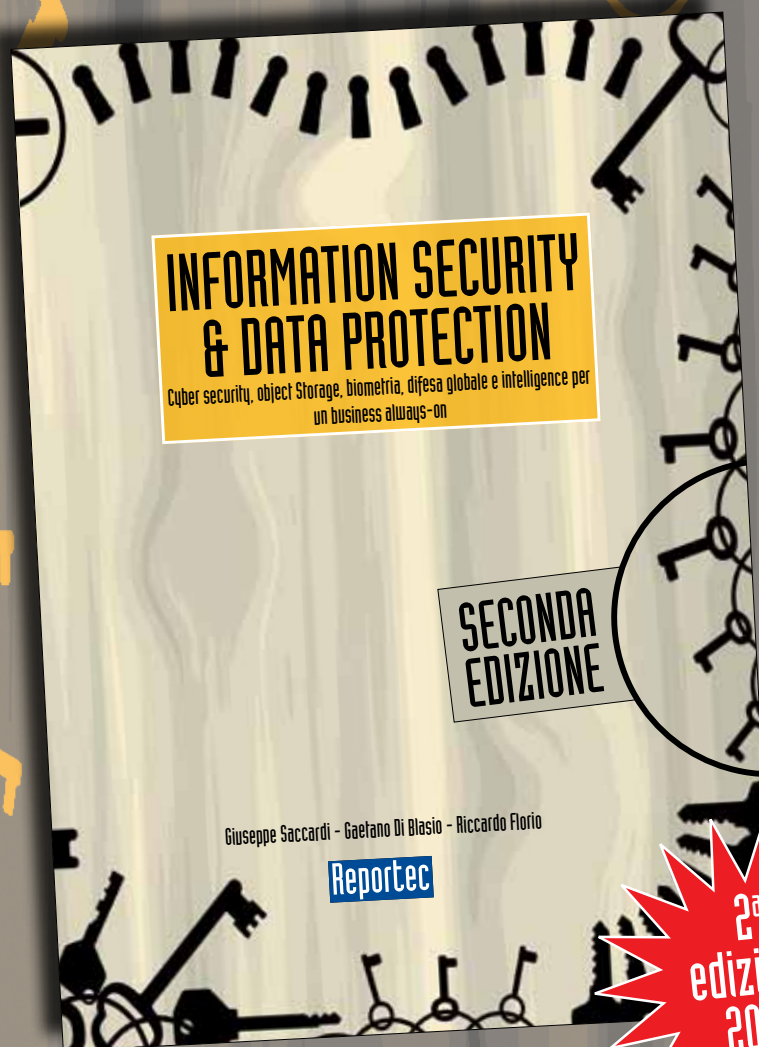
Controllo centralizzato per la cifratura USB con Endpoint Protector

PROTAGONISTI

pag. 19

Gastone Nencini, Trend Micro: difendersi dal furto dei dati

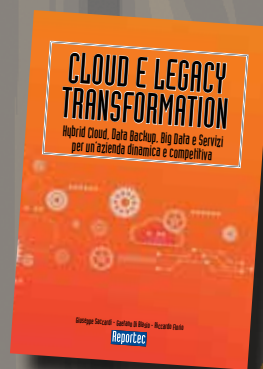
È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION



Il libro è acquistabile al prezzo di 48 euro (più IVA 22%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

CYBER ATTACK

COSTA 4 MILIONI DI DOLLARI UN INCIDENTE DI CYBER SECURITY

Gli attacchi andati a buon fine nel 2015 sono aumentati del 64% rispetto all'anno precedente e cresce anche il costo medio che arriva a 158 dollari per record compromesso

di Gaetano Di Blasio

Aumentano i costi medi delle violazioni alla sicurezza dei dati secondo lo studio annuale del Ponemon Institute, sponsorizzato da IBM: più precisamente la crescita è del 29% rispetto al 2013, che porta il costo medio di un cyber security incident a 4 milioni di dollari (in Italia: 3,26 milioni di dollari). In settori altamente regolamentati i costi sono più

alti, come in quello sanitario, dove il costo per record è arrivato a quota 355 dollari: 100 dollari in più rispetto al 2013.

In generale gli attacchi sono sempre più sofisticati e aumentano in numero, così pure cresce la quota di quelli che vanno a buon fine: più 64% nel 2015 rispetto il 2014, con un costo medio per record



compromesso arrivato a 158 dollari. In Italia siamo passati dai 141 del 2014 ai 146 del 2015, per giungere ai 156 nel 2016.

Ridurre i costi

Ci sono aziende che sono riuscite a far ridurre tali costi, grazie a interventi adeguati. Il costo viene calcolato sommando diversi fattori, tra cui i tempi di risposta e la pianificazione. Secondo gli autori dello studio, la presenza di un team di risposta agli incidenti è il fattore che più ha inciso sulla riduzione dei costi di una violazione dei dati - permettendo alle aziende di risparmiare in media quasi 400mila dollari (o 16 dollari per record).

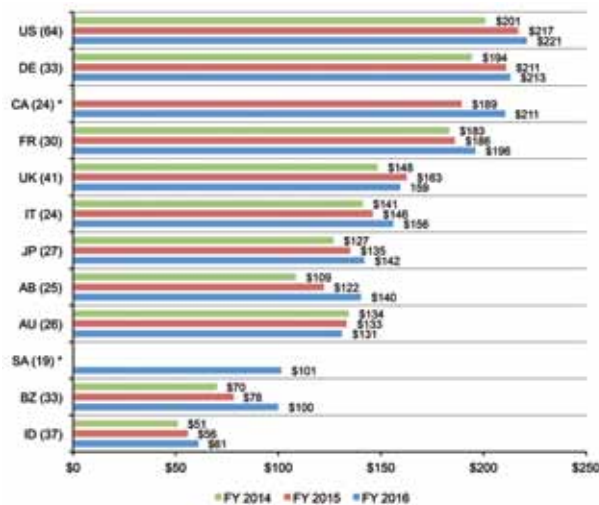
Gli analisti di Ponemon, nello specifico, ritengono che le attività di risposta agli incidenti, quali le indagini, le comunicazioni, le spese legali e i mandati

delle autorità di regolamentazione, rappresentano il 59% del costo di una violazione dei dati.

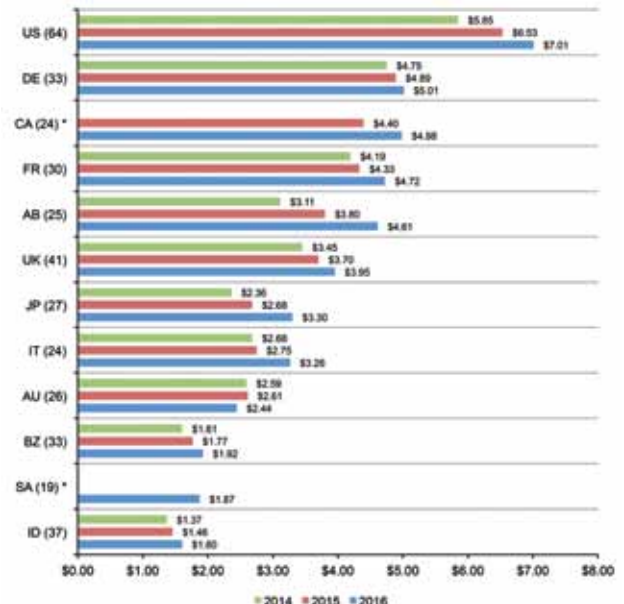
Si sospetta, quindi, che il costo medio elevato sia in buona parte dovuto all'assenza di piani e politiche per l'incident response presso ben il 70% delle aziende coinvolte nello studio.

La mancanza di pianificazione sarebbe, dunque, più costosa della struttura per la pianificazione stessa. Questo perché, in caso di incidente, il processo di risposta "improvvisato" risulta oneroso, anche per la sua complessità. Infatti, evidenziano gli analisti del Ponemon Institute, le attività richieste in questo caso comprendono:

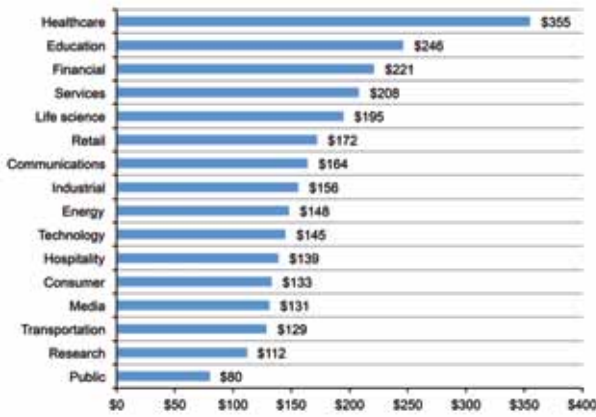
- Collaborare con esperti della sicurezza interni o esterni per identificare rapidamente l'origine della violazione e arrestare un'ulteriore perdita di dati.
- Dichiarare la violazione ai responsabili delle



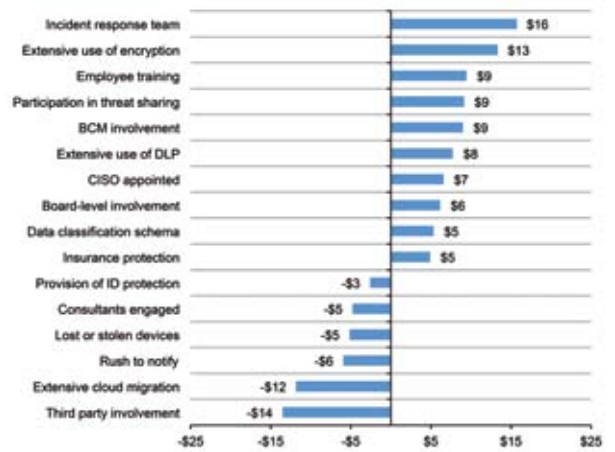
Costo medio in dollari per record violato in ciascuna nazione nei tre anni della ricerca. La media complessiva è stata: 145 dollari nel 2014, 154 dollari nel 2015 e 158 dollari nel 2016 (i dati storici non sono disponibili per tutte le nazioni)



Costo medio di un cyber incident per nazione (valori in milioni di dollari)



Costo medio per record violato in funzione del settore economico



Impatto di alcuni fattori, in negativo o in positivo, sul costo di una violazione

autorità governative e/o degli enti regolatori competenti, rispettando scadenze specifiche al fine di evitare potenziali multe.

- Comunicare la violazione a clienti, partner e stakeholder.
- Allestire l'eventuale supporto telefonico necessario e i servizi di monitoraggio del credito per i

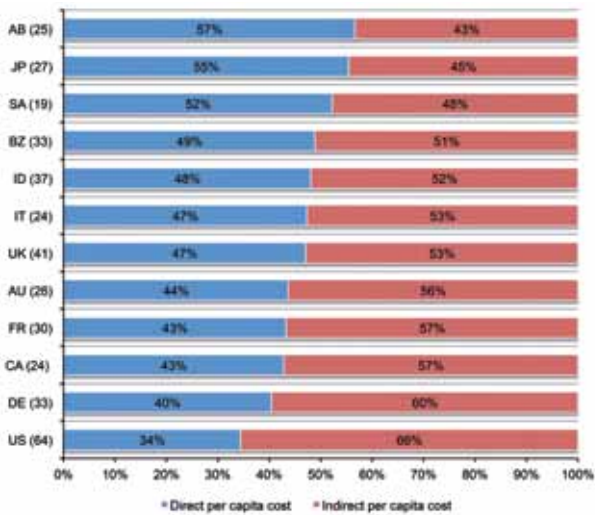
clienti interessati.

Ciascuna di tali azioni implica numerose ore d'impegno, le quali vengono sottratte alle normali attività e responsabilità quotidiane. I team di risposta sono preparati e quindi attuano più velocemente tali processi, con minor rischio di commettere errori e maggiori garanzie di affrontare tutti gli aspetti

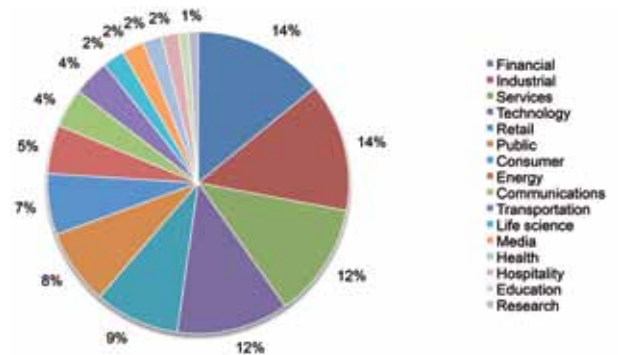
Analisi del costo dovuto a una violazione dei dati

Lo studio annuale "Cost of a Data Breach" esamina i costi diretti e indiretti per un singolo incidente. Metodologicamente, lo studio viene condotto attraverso approfondite interviste con, quest'anno 383 aziende in varie parti del mondo (Arabia Saudita, Australia, Brasile, Canada, Emirati Arabi, Francia, Germania, Giappone, India, Italia, Regno Unito, Stati Uniti, Sudafrica), tenendo conto dei costi associati alle attività di risposta alle violazioni, nonché il danno d'immagine e il costo per la perdita di business.

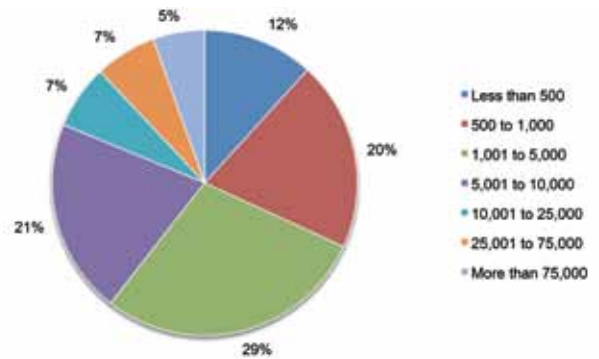
Sono vari anni che il Ponemon Institute conduce queste analisi, avendo coinvolto oltre 2mila imprese di tutti i settori economici, tanto che Larry Ponemon, fondatore della società di ricerca, dà ormai per assodato che le violazioni rappresentano un costo sistematico per le imprese: «Le evidenze dimostrano che si tratta di un costo permanente, con cui le organizzazioni devono essere pronte a confrontarsi e che devono inserire nelle loro strategie di protezione dei dati».



Incidenza percentuale di costi diretti e indiretti in una violazione per nazione



Distribuzione del campione per industria



Distribuzione del campione per numero di dipendenti

delle attività di sicurezza e del ciclo di vita della risposta, dall'aiuto nella risoluzione dell'incidente, ai problemi specifici per il settore d'industria, fino alla conformità normativa.

Va, inoltre, considerato che specifiche tecnologie possono automatizzare il processo di risposta agli incidenti.

201 giorni, il tempo medio per rilevare una violazione

Tornando allo studio, è stato riscontrato che tempi più lunghi di rilevamento e contenimento di una violazione dei dati determinano un aumento dei costi di risoluzione: le violazioni identificate in meno di 100 giorni costano alle aziende in media 3,23 milioni di dollari, mentre quelle individuate dopo i 100 giorni costano in media 4,38 milioni di dollari, oltre 1 milione di dollari aggiuntivi.

Secondo lo studio, il tempo richiesto in media per identificare una violazione è stato stimato in 201 giorni, mentre il tempo medio di contenimento è stato stimato in 70 giorni. A preoccupare, però, è anche il dato minimo. Infatti, i più veloci, hanno impiegato comunque 20 giorni a rilevare un attacco andato a buon fine, mentre i peggiori ci hanno messo 596 giorni.

Anche in questo caso, le imprese preparate, cioè quelle che hanno in esercizio processi di business continuity management, sono state più rapide, rilevando, in media, le violazioni 52 giorni prima e impiegando 36 giorni meno per contenerle, rispetto a chi non ha strutturato una strategia di business continuity.

GARANTIRE LA SICUREZZA DELLE INFRASTRUTTURE CRITICHE

Nel corso degli anni i sistemi di controllo industriale sono diventati più aperti verso il mondo esterno ed è cresciuta la loro vulnerabilità agli attacchi dalla rete. In uno scenario in cui cyber crime e terrorismo sono sempre più vicini, preoccuparsi della sicurezza delle infrastrutture critiche diventa quanto mai importante

di Riccardo Florio

Le infrastrutture critiche come, per esempio impianti di generazione di energia elettrica, sistemi di trasporto, raffinerie di petrolio, industrie chimiche e impianti di produzione, sono in generale complessi distribuiti e di grandi dimensioni.

Gli operatori dell'impianto devono continuamente monitorare e controllare molte sezioni differenti dell'impianto per garantirne il corretto funzionamento e, durante gli ultimi decenni, queste operazioni di

comando remoto e controllo sono state agevolate dallo sviluppo delle tecnologie di rete e dall'avvento dei sistemi di controllo industriale (Industrial Control System, in sigla ICS).

Gli ICS sono sistemi e reti di controllo e comando progettate per supportare i processi industriali. Il termine comprende diversi tipi di sistemi di controllo utilizzati all'interno della produzione industriale; il più vasto sottogruppo di ICS è quello dei sistemi



Scada (Supervisory Control and Data Acquisition) a cui si affiancano i Distributed Control System (DCS) e altre configurazioni di sistemi di controllo più piccole quali PLC (Programmable Logic Controller) che si trovano anche all'interno dei settori industriali più disparati.

Vulnerabilità cresciuta nel tempo

Nel corso degli anni gli ICS sono passati attraverso una trasformazione significativa, evolvendo da sistemi proprietari che operavano in modo isolato, verso architetture aperte basate su tecnologie standard e altamente interconnesse con altre reti aziendali e Internet.

Attualmente, i prodotti ICS sono, per lo più, basati su piattaforme standard di sistemi "embedded" e spesso utilizzano software di tipo commerciale. Tutto ciò ha determinato un'importante riduzione dei costi, semplificato l'utilizzo e consentito il controllo e monitoraggio da ogni località. Tuttavia, la connessione a reti intranet e di comunicazione ha determinato un incremento nella vulnerabilità rispetto ai tipici attacchi di rete.

Va rimarcato che i sistemi ICS, sebbene simili nelle funzioni ai sistemi di ICT, differiscono notevolmente da questi ultimi nel modo di interpretare l'esigenza di sicurezza. La prima priorità dei sistemi IT di sicurezza è tipicamente la protezione dei dati mentre nei dispositivi ICS si tende a privilegiare l'affidabilità e l'accessibilità dei dati per non compromettere la produttività ed evitare qualsiasi forma di latenza che potrebbe causare inconvenienti. Considerare allo stesso modo gli aspetti di sicurezza dei sistemi ICS e di quelli IT può portare a falle di sicurezza; una profonda comprensione delle minacce alla sicurezza di sistemi di controllo industriali e delle tecnologie

correlate è dunque necessaria al fine di inquadrare gli aspetti distintivi e gestire correttamente il rischio separandolo da quello della sicurezza IT.

Solitamente i sistemi ICS non prevedono la presenza di soluzioni anti malware ed è quindi opportuno predisporre strumenti integrati capaci di intervenire in modo automatizzato su più fronti, affiancandogli un sistema di modellazione delle minacce adeguato a ogni specifica infrastruttura.

Un rischio da non sottovalutare

In uno scenario in cui il "cyber crime" e il terrorismo sono sempre più accumulati da metodiche e finalità, il tema di garantire la sicurezza delle infrastrutture critiche diventa quanto mai importante.

La possibilità che un malware si inserisca all'interno dei sistemi di controllo e automazione apre scenari di rischio tanto importanti quanto facilmente prevedibili. Allo stesso livello di rischio sono esposte anche le realtà industriali e manifatturiere, che potrebbero trovarsi a dover fronteggiare il blocco dell'intera catena di produzione nel caso i propri sistemi di controllo venissero compromessi.

Gli esempi ci sono già e minacce quali Stuxnet e Flame hanno già segnato la loro impronta nella storia del "cyber crime". In particolare, Stuxnet è considerato uno dei codici malware più sofisticati che sia mai stato scritto, tanto che la sua analisi e comprensione ha richiesto molti mesi. Sono stati identificati file infetti con questo malware che era presente in modo dormiente da diversi anni, in attesa di essere sfruttato per attacchi su larga scala. Un altro problema di cui tenere conto è che le macchine SCADA sono gestite e mantenute da terze parti e difficilmente si ha la possibilità di esercitare un'azione di controllo diretta sui loro processi di

I sistemi Scada

Il termine Scada, acronimo di Supervisory Control And Data Acquisition, si riferisce a un sistema di gestione e controllo distribuito per il monitoraggio di sistemi fisici.

Tipicamente, i sistemi di tipo Scada sono costituiti da sensori, che effettuano misurazioni di grandezze fisiche, microcontrollori. Tipicamente, i sistemi di tipo Scada sono utilizzati come sistemi di controllo in ambito industriale per il monitoraggio e controllo infrastrutturale o di processi industriali e sono composti da sensori che effettuano misurazioni di grandezze fisiche, microcontrollori (per esempio PLC), una rete che collega i microcontrollori con il supervisore, un computer con funzione di supervisore che raccoglie i dati e ne estrae le informazioni utili e che fa scattare allarmi in caso di malfunzionamenti.

Un sistema Scada utilizza una rete di telecomunicazioni di tipo geografico (WAN); sistemi simili, ma basati su una rete di comunicazione locale (LAN) sono propriamente definiti DCS (Distributed Control System): tipici esempi sono i sistemi di controllo e supervisione di impianti industriali. I sistemi DCS si collocano a un livello superiore potendo, oltre che supervisionare, anche comandare i sistemi di automazione, cosa che ai sistemi Scada è, invece, inibita.

sicurezza. Se non si mette a disposizione dei manutentori un sistema efficace e semplice per effettuare un controllo in linea della macchina, il rischio di introdurre malware su uno di questi dispositivi diventa elevato.

Nonostante tutto ciò, l'attenzione verso il tema della sicurezza dei sistemi ICS resta ancora, inspiegabilmente, bassa.

A fronteggiare questi scenari sono chiamati, dunque, non solo i produttori di tecnologie di sicurezza, ma anche i rappresentanti del mondo industriale e delle istituzioni governative.

Sei raccomandazioni dall'Enisa

La European union agency for network and information security (Enisa) è un centro di competenza sulla sicurezza delle informazioni e delle reti per l'Unione Europea, i suoi stati membri, il settore privato e, in generale, i cittadini europei.

Dall'Enisa, all'interno del report dal titolo "Analysis of ICS-SCADA Cyber Security Maturity Levels



Migrare i dati Scada sul cloud ? Una scelta possibile

La possibilità di collegare Scada e cloud trova crescente attenzione in relazione alle opportunità di riduzione dei costi, ridondanza dei sistemi e benefici in termini di continuità operativa. Le ragioni per scegliere una siffatta migrazione possono essere ricondotte a quelle che, in generale, riguardano altri sistemi di tipo critico da cui i dispositivi Scada non si differenziano molto. D'altronde, il mercato ha ormai dimostrato che il cloud non è una moda passeggera e che i possibili benefici in termini di costi, sicurezza integrata, ridondanza e uptime sono concreti.

La migrazione dei dispositivi Scada verso il cloud è, potenzialmente, in grado di risolvere questioni critiche correlate al tempo di uptime e alla ridondanza richieste negli ambienti ICS. Inoltre, il ricorso al cloud semplifica l'accesso ai dati che diventa possibile da qualsiasi postazione connessa a Internet. L'utilizzo del cloud potrebbe anche fornire un aiuto per far fronte alle crescenti esigenze di velocità nell'accesso alle informazioni dei dispositivi di controllo industriale. La capacità di predisporre rapidamente un'infrastruttura rende anche la ridondanza un problema facile da risolvere con l'utilizzo di cloud. Inoltre, la flessibilità offerta da questo metodo consente aggiornamenti dei sistemi più veloci nel caso di mancanza di spazio su disco rigido o di un utilizzo eccessivo della CPU.

Le aziende che hanno usato il cloud sono state in grado di risolvere problemi di disaster recovery in meno tempo rispetto a quelle che non utilizzano il cloud. Questo è probabilmente attribuibile alla risoluzione dei possibili problemi legati all'hardware. Inoltre, anche gli aggiornamenti automatici possono essere direttamente attribuiti all'uso del cloud. La maggior parte dei cloud service provider si fanno carico della manutenzione del server, tra cui il "rollout" degli aggiornamenti di sicurezza. L'uso del cloud permette anche di liberare tempo e risorse che gli amministratori IT possono utilizzare per altri progetti.

in Critical Sectors", proviene la seguente serie di raccomandazioni che punta a indicare la direzione su cui intervenire per migliorare il livello di maturità nelle azioni di contrasto alle minacce alle infrastrutture critiche.

- Allineare gli sforzi ICS-Scada con strategie nazionali di sicurezza informatica e attività legate alla Critical Information Infrastructure Protection (CIIP).
- Sviluppare standard di sicurezza e best practice specifiche per la protezione dei sistemi ICS.
- Standardizzare la condivisione delle informazioni tra i settori critici e le istituzioni europee legate a incidenti di sicurezza informatici ICS.
- Costruire una consapevolezza sui rischi legati ai sistemi di controllo industriali che non coinvolga solo gli operatori che gestiscono le infrastrutture critiche, ma anche decision maker del mondo industriale e della politica.
- Promuovere competenze con corsi di formazione sulla sicurezza dei sistemi ICS e programmi educativi.
- Promuovere e sostenere la ricerca sulla sicurezza dei sistemi ICS-Scada e predisporre test comuni coinvolgendo gli esperti del settore e i vendor di sicurezza.

KASPERSKY LAB E LA SICUREZZA DEI SISTEMI INDUSTRIALI

Una soluzione specializzata per proteggere le infrastrutture critiche e l'integrità dei processi tecnologici nei nuovi ambienti integrati manifatturieri

di Gaetano Di Blasio

Kaspersky Lab ha sviluppato una soluzione per la protezione delle infrastrutture critiche e degli ambienti industriali.; si tratta di Kaspersky Industrial CyberSecurity. I sistemi ICS (Industry Control System) richiedono continuità ecco perché occorrono soluzioni di sicurezza conformi alla regolamentazione e Kaspersky Industrial CyberSecurity è stata progettata per fornire un approccio unificato alla sicurezza informatica per gli ambienti industriali, combinando le migliori tecnologie dell'azienda russa, servizi e intelligence in un solo pacchetto. In particolare impostazioni altamente personalizzabili di Kaspersky Industrial CyberSecurity permettono di configurare la soluzione in piena conformità con i requisiti di diversi settori di produzione, permettendo alla soluzione di essere efficacemente integrata all'interno dell'attuale network ICS di un'organizzazione.

«Tutte le nostre tecnologie sono state testate dai maggiori vendor ICS. Kaspersky Industrial CyberSecurity è stato integrato in numerosi progetti, compresi il terminal petrolchimico Vars e al colosso delle raffinerie di petrolio Taneco, che hanno scelto



*Morten Lehn,
General Manager
di Kaspersky Lab
Italia*

Kaspersky Lab per proteggere le loro reti industriali», sottolinea Morten Lehn, General Manager di Kaspersky Lab Italia.

Prevenire le minacce anche con la formazione

La nuova soluzione protegge dalle minacce informatiche i livelli della rete ICS più vulnerabili agli attacchi. Più precisamente, Kaspersky Industrial CyberSecurity fornisce una combinazione di tecnologie di sicurezza convenzionali, adattate per gli ambienti ICS, compresa la protezione anti-malware, il whitelisting e la funzionalità di valutazione delle vulnerabilità. I programmi di includono: sicurezza di base nei sistemi ICS, attacchi di ingegneria sociale alle infrastrutture critiche e altro ancora. I servizi specialistici includono la valutazione della sicurezza informatica e i test di penetrazione. I servizi di incidenti response aiutano a localizzare l'intrusione, mitigarne le conseguenze, impedire agli aggressori di penetrare ulteriormente nell'infrastruttura, prevenire successivi attacchi all'azienda e sviluppare un piano di risposta agli incidenti per il futuro.

LE LINEE GUIDA PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

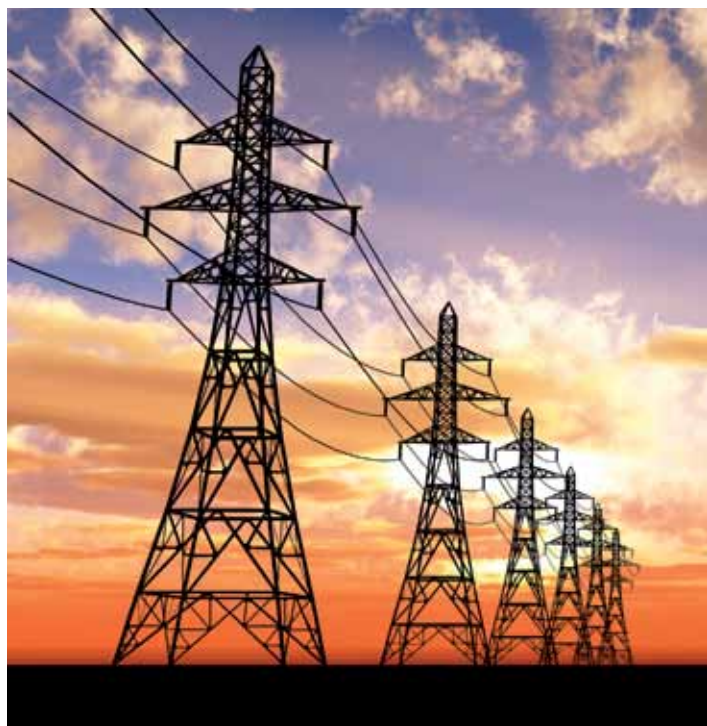
Fortinet propone 10 "guidelines" per far fronte agli incidenti di sicurezza in ambito industriale che, nella maggior parte dei casi, nascono da problematiche interne non volontarie

a cura della Redazione

Le macchine e la tecnologia utilizzate per gestire e mettere in funzione infrastrutture critiche quali centrali idroelettriche, stabilimenti petroliferi, acquedotti e così via non sono state progettate per essere connesse a reti remote o pubbliche. L'isolamento, anche fisico, di tali sistemi ha portato in molti casi a non considerare la sicurezza informatica con la dovuta attenzione. L'avvento dell'era cosiddetta dell'Industry 4.0 ha però determinato una maggiore interconnessione di questi ambienti e la proliferazione di standard aperti ha contribuito ulteriormente a incrementarne la vulnerabilità.

I rischi di sicurezza in ambito industriale sono seri e, oltre all'ampiamiento della superficie di attacco, è importante fare fronte agli incidenti causati da problematiche interne non volontarie, come errate configurazioni software o protocolli di rete malfunzionanti che, secondo Fortinet, rappresentano quasi l'80% del totale.

«Un approccio maggiormente olistico alla sicurezza diventa necessario per proteggersi sia dagli attacchi mirati provenienti dall'esterno sia dall'errore umano che può verificarsi internamente - spiega Filippo



Monticelli, Country Manager di Fortinet Italia - «Risolvere le problematiche di sicurezza dei sistemi di controllo industriale richiede una soluzione in grado di unire il meglio delle funzionalità di sicurezza delle tecnologie operative di rete con una comprensione profonda di processi e protocolli legati ai sistemi di controllo industriali».

10 punti per una difesa efficace

Il suggerimento di Fortinet è che, sebbene le aziende non possano prevedere ogni minaccia, possono affrontare gli aspetti che possono controllare. Per questo motivo il vendor ha recentemente definito le seguenti 10 linee guida per aiutare le aziende a valutare

le vulnerabilità della propria tecnologia operativa.

1. **Identificare le risorse critiche da proteggere:** è il primo e fondamentale passo, propedeutico a qualsiasi tipo di intervento e per nulla scontato.
2. **Definire protocolli per la gestione dei per-**



messi o per l'accesso ai controlli: ora che le tecnologie operative sono interconnesse con i sistemi informativi, devono tenere il passo delle best practice di sicurezza e determinare i privilegi appropriati per gli utenti autorizzati è tanto importante quanto bloccare accessi non autorizzati.

3. **Aggiornare regolarmente i sistemi operativi hardware e software:** alcuni sistemi operativi sono antecedenti al concetto stesso di cyber-sicurezza ed è, pertanto, indispensabile assicurarsi che siano compatibili con le moderne difese di base, quali antivirus e tecnologie di scansione.
4. **Occuparsi con regolarità di aggiornamenti e patch:** molte attività non possono permettersi

interruzioni e costi associati alle patch, ma il continuo rinvio degli aggiornamenti è causa di vulnerabilità più ampie nella sicurezza.

5. **Identificare dispositivi di telemetria non protetti e dotati di indirizzo IP:** è importante tenere presente che i dati su apparati quali sensori e manometri possono essere manipolati, compromettendo la sicurezza e l'affidabilità di tutto il sistema.
6. **Adottare best practice in tema di coding:** l'adozione di software integrato e spesso personalizzato, scritto dedicando poca attenzione alle tecniche di sicurezza raccomandate, lascia i sistemi industriali esposti a possibili attacchi.
7. **Seguire procedure standard per il logging degli eventi:** predisporre un processo per effettuare report sugli eventi di sistema fornisce dati che consentono di rilevare le irregolarità e implementare misure di sicurezza efficaci.
8. **Tenere sotto controllo produzione delle componenti e supply chain:** senza monitoraggio e governance appropriati, gli apparati potrebbero risultare compromessi ancor prima di essere installati.
9. **Implementare un'efficace segmentazione di rete:** in assenza di un'opportuna segmentazione, dati e applicazioni compromessi possono passare da un segmento all'altro e i criminali che riescono a violare le difese perimetrali sono così in grado di spostarsi in incognito attraverso l'intera rete.
10. **Definire un piano di operational recovery:** nel malaugurato caso di disastro, ogni azienda richiede procedure documentate per valutare i danni, riparare macchine e sistemi e ripristinare le operazioni; esercitazioni abituali consentono agli operatori di effettuare il ripristino in modo più rapido ed efficiente quando si verificano situazioni di questo tipo.

RAD, Check Point e CIE Telematica collaborano per garantire la sicurezza delle infrastrutture di rete delle public utility e degli ambienti Scada

di Giuseppe Saccardi

La migrazione in atto a livello di infrastrutture industriali nel quadro di quello che viene riferito come Industry 4.0, accompagnata dalla diffusione dell'IoT, sta ponendo serie sfide ai gestori delle reti che collegano i sensori e gli apparati di controllo. Una ulteriore sfida è posta dall'esigenza di erogare servizi a qualità garantita sia nell'ambito delle public utilities quali l'energia, il gas o il settore idrico, che nei trasporti pubblici e nella PA.

Si tratta di settori che per la loro criticità necessitano di una elevata sicurezza nelle operation e la garanzia che i dati che viaggiano in rete siano protetti, inalterabili e certi nella loro consegna.

Quello che serve in sostanza, evidenzia Luigi Meregalli, general manager di CIE Telematica e storicamente rappresentante unico di RAD in Italia, sono sistemi di Service Assured Networking (SAN) pensati specificatamente per essere applicati in infrastrutture critiche.

Esistono però diversità a seconda del settore e per questo RAD si è mossa su due diverse linee che si sono consolidate in due principali categorie di soluzioni.

RAD SecFlow 2



Soluzioni per mercati verticali e per "power utility"

La prima risponde alle esigenze delle infrastrutture critiche di mercati verticali quali le citate Utility, il trasporto e la PA. Comprende soluzioni di operational WAN (con apparati Megaplex), "automation backhaul" (con la soluzione SecFlow), wireless point-to-point e point-to-multipoint (con la famiglia Airmux), teleprotezione (le soluzioni Megaplex), rugged LAN per ambienti critici (sempre con SecFlow) e di broadband mobility (Airmux).

Per quanto riguarda le applicazioni rivolte alle power utility, RAD ha posizionato i propri prodotti nella distribuzione e nella trasmissione di energia concentrandosi su quanto non coinvolge il lato della generazione.

Si tratta, evidenzia Meregalli, di interventi a largo respiro volti ad assicurare sia le corrette funzioni di rete, che la sicurezza delle informazioni e l'operatività delle infrastrutture anche in ambienti estremi, il tutto in linea con le normative che sottostanno alle soluzioni Scada.

Per mitigare o annullare del tutto i rischi di attacchi,



RAD ha stretto un accordo con Check Point per sfruttarne nei suoi apparati, come per esempio la famiglia SecFlow, i criteri e le tecnologie per la sicurezza delle reti e delle applicazioni.

In particolare, l'accordo è relativo alla integrazione nel portfolio di prodotti SAN di RAD della soluzione ICS Security Gateway di Check Point. Il risultato è che diventa possibile disporre di una soluzione che gestisce in modo sicuro tutti gli accessi elettronici al perimetro di sicurezza elettronico (ESP) delle sottostazioni di un impianto e protegge l'asset interno al perimetro da attacchi interni o esterni, compresi i classici "man-in-the-middle", sessioni di hijacking", source-spoofing e DDoS.

RAD SecFlow2 per la sicurezza delle infrastrutture

SecFlow2 è una soluzione che permette di connettere la tecnologia Scada ai dispositivi RAD di sicurezza di rete della famiglia SecFlow attraverso la porta seriale in modo da creare un tunnel IPsec criptato nella rete VPN che comunica con un firewall Checkpoint. Va osservato che i dispositivi SecFlow sono soluzioni

Switch/Router in versione rugged e "Scada aware", disponibili sia in versione compatta o in versione modulare. Tra le funzioni che realizzano vi sono: autenticazione, autorizzazione, cifratura, il tutto su reti fisse in rame o fibra e su reti mobili, sia a livello 2 che 3. Specificatamente per la sicurezza, SecFlow-2, è un prodotto che incorpora la funzione di Firewall che permette di disporre a livello di rete delle funzioni di sicurezza per applicazioni Scada (IEC 104, Modbus TCP, e DNP3 DCP).

Il dispositivo monitorizza i comandi Scada tramite la deep packet inspection in modo da verificare se essi corrispondono o meno agli scopi dell'applicazione. A questo aggiunge la funzione di gateway VPN con due diversi modi operativi: connessione tra siti con tunnel IPsec; accesso remoto SSH (Secure SHell).

In pratica, la connessione trasparente e sicura di reti Ethernet a livello 2 e 3 è assicurata tramite VPN intrasito basate su tunnel GRE (Generic Routing Encapsulation) su link criptati IPsec. Per l'accesso remoto la sicurezza è assicurata tramite un tunnel SSH criptato, l'autenticazione dell'utente e specifiche autorizzazioni e credenziali di accesso.

ACEA DISTRIBUZIONE, PIÙ SICURO CON LE SOLUZIONI DI CHECK POINT

Il fornitore pubblico italiano ha adottato le soluzioni 1200R per migliorare la protezione sulle reti Scada

a cura della Redazione

Acea Distribuzione, parte del Gruppo Acea, è una delle principali multi-utility pubbliche italiane per la fornitura idrica e di energia. L'esigenza di mettere in sicurezza le proprie infrastrutture critiche, le reti Scada e i sistemi di controllo industriali (ICS) ha portato l'azienda alla scelta della soluzione di protezione per il gateway Check Point 1200R. La soluzione è stata implementata all'interno dell'infrastruttura di rete aziendale preesistente dal system integrator DGS Group. La scelta di Check Point è arrivata dopo una preselezione e i responsabili di Acea hanno apprezzato la capacità della soluzione 1200R di funzionare in ambienti operativi estremi, compresi i siti di confronto e distribuzione dell'energia primari e secondari, ma anche di soddisfare alcuni requisiti tecnici specifici. In particolare, la soluzione Check Point 1200R integra anche l'infrastruttura di supporto decisionale per la cyber-sicurezza Panoptesec.

Acea è stata così la prima azienda a utilizzare il servizio Panoptesec per centralizzare i dati e le risorse provenienti dai propri partner e dai fornitori, facendo così confluire informazioni scaturite da vari sistemi di difesa di cyber-sicurezza e indagine,

L'appliance di sicurezza Check Point 1200R



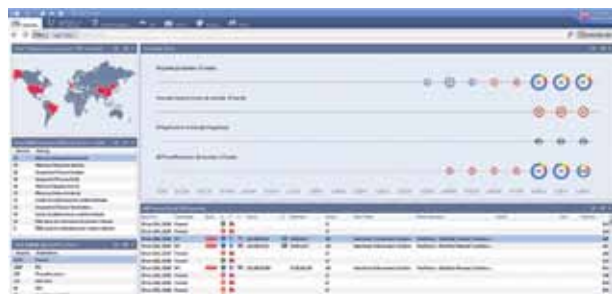
compresi firewall, IPS / IDS, Silent Defense e Syslog al fine di semplificare le analisi e il monitoraggio. «Ci tenevamo a difendere i nostri sistemi Scada interni ed esterni e i relativi centri Command&Control - precisa Andrea Guarino, ICT security, privacy and compliance manager di Acea -. Il nostro problema era riuscire a rilevare e bloccare tutti gli attacchi "normali" alle nostre reti, oltre agli attacchi che, invece, erano mirati alle reti Scada e ai dispositivi industriali. Inoltre, volevamo la certezza della completa visibilità delle sequenze di comando Scada, inviate e ricevute sulle reti controllate, e di riuscire a registrarle per scopi investigativi e di analisi. La soluzione Check Point è stata l'unica a soddisfare tutti i nostri criteri».

Check Point 1200R

Check Point 1200R è un'appliance di sicurezza di tipo "rugged" appositamente predisposta per gli ambienti industriali più estremi e per l'utilizzo remoto. L'appliance 1200R soddisfa le specifiche IEEE 1613 e IEC 61850-3 per il calore, le vibrazioni e l'immunità ai campi elettromagnetici ed è in grado di operare all'interno di un range di temperature compreso tra

-40 °C e + 75 °C senza ventole né alcuna parte in movimento. La soluzione di Check Point integra funzioni di firewall, IPS, application control, antivirus e anti-bot e fornisce visibilità e controllo granulare del traffico Scada per prevenire attacchi a reti, dispositivi e processi logic. Attraverso il Check Point Application Control, la soluzione fornisce un supporto per i protocolli specializzati Scada e ICS per oltre 500 comandi e supporta più di 280 firme IPS specifiche per le reti Scada. Inoltre, attraverso la console SmartEvent di Check Point è possibile consolidare in un'unica postazione centralizzata le attività di monitoraggio, logging, reportistica e analisi degli eventi per conseguire una completa visibilità e generare report completi sul traffico.

«La soluzione di Check Point ci offre una sicurezza avanzata e ha migliorato la nostra capacità di individuare e reagire a potenziali vulnerabilità - ha aggiunto Guarino -. Adesso abbiamo una prospettiva più chiara dei flussi di comando e delle informazioni utilizzate dai nostri sistemi Scada e dai sistemi di controllo industriali».



Check Point SmartEvent

Il progetto Panoptesec

Nonostante la necessità ben nota per il monitoraggio continuo dei sistemi ICT al fine di individuare le vulnerabilità e attacchi, come pure la necessità di risposta rapida ai problemi, molte restano le lacune di sicurezza all'interno delle moderne reti e sistemi.

Panoptesec è un'iniziativa, finanziata dall'Unione Europea, che affronta la sfida del rilevamento delle vulnerabilità e dei possibili attacchi a dati sensibili, reti e servizi, per fornire gli strumenti per gestire gli incidenti di sicurezza. Il termine prende spunto da Panoptes, parola greca che significa "vedere tutto".

Panoptesec è un consorzio che ha come obiettivo quello di realizzare l'omonimo prototipo di un sistema di supporto decisionale per la difesa dai cyber-attacchi, che adotti un approccio basato sul rischio per automatizzare le operazioni di difesa dal cyber crime, riuscendo a tener conto della natura dinamica delle tecnologie dell'informazione e delle comunicazioni e della continua evoluzione degli attacchi informatici.

Il prototipo Panoptesec affronta queste sfide utilizzando motori di analisi automatizzata per valutare in modo proattivo e reattivo le debolezze di sistema, individuare potenziali percorsi di attacco, fornire un elenco organizzato per priorità delle azioni di risposta e mettendo a disposizione un mezzo per gestire e reagire automaticamente a questo tipo di incidenti.

Il prototipo sarà in grado di supportare le notifiche di violazioni e migliorare la consapevolezza della situazione, fornendo contestualmente un supporto al processo decisionale richiesto dal personale di sicurezza. Panoptesec metterà a disposizione le funzionalità richieste attraverso una serie di tecnologie integrate, modulari e basate su standard.



ENDPOINT PROTECTOR: CONTROLLO CENTRALIZZATO E CIFRATURA USB

CoSoSys ha aggiornato Endpoint Protector DLP con la funzione di gestione remota di cifratura di dispositivi USB per Windows e Mac OS X

di Giuseppe Saccardi



CoSoSys, produttore di soluzioni Data Loss Prevention e Mobile Device Management, ha annunciato il rilascio della funzione USB Enforced Encryption per Endpoint Protector 4 per incrementare la sicurezza dei dati copiati nei dispositivi USB. Recenti ricerche mostrano che 22,266 chiavette USB e 937 telefonini sono lasciati ogni anno nelle lavanderie di indumenti. Altri posti dove vengono dimenticati questi sono treni, ristoranti, taxi e altro. Senza cifratura i dati contenuti possono finire in mani sbagliate.

«La nuova funzione di Cifratura Forzata può costituire un cambio di passo significativo per le organizzazioni che hanno dipendenti autorizzati a gestire informazioni aziendali riservate. Questo aggiornamento garantisce un uso sicuro dei dispositivi USB grazie alla gestione remota e attiva in caso di dispositivo perso o rubato», ha commentato Roman Foeckl, CEO e fondatore di CoSoSys. Sotto il profilo operativo l'aggiornamento USB Enforced Encryption permette agli amministratori IT di gestire remotamente e forzare la cifratura nei dispositivi USB connessi a computer che abbiano installato l'agent di Endpoint Protector DLP.

Quando questa funzione è attivata, qualora un utente connettesse il dispositivo USB, verrà automaticamente installato il software di cifratura, protetto da password. Ogni volta che l'utente cercherà di copiare dati nel dispositivo USB, il software di cifratura si attiverà e trasferirà i dati in modalità cifrata.

Per promuovere la consapevolezza e la comprensione, la nuova funzione USB Enforced Encryption permette al team IT di inviare messaggi personalizzati, compresi avvisi di cambio password o altre informazioni.

L'aggiornamento è disponibile con Endpoint Protector versione 4.4.1.0 e si trova nella sezione Live Update della consolle di gestione.

«Con il rilascio della nuova funzione siamo in grado di aumentare notevolmente la sicurezza dei dispositivi USB che, se persi o rubati, garantiscono l'impossibilità di furto dati. Questo è sicuramente un passo importante verso la quasi totale sicurezza dei dispositivi USB, anche grazie alla gestione da remoto e a un efficace sistema di recovery», ha commentato Maurizio Moroni, responsabile della divisione security di Partner Data.

The World is Your Workplace

FUJITSU

shaping tomorrow with you



Fujitsu LIFEBOOK S936 Massima sicurezza con sensore palm vein integrato

Il nuovo dispositivo leggero e touch Fujitsu LIFEBOOK S936 è il compagno ideale per chi viaggia spesso. Il vano modular bay garantisce tutta la flessibilità necessaria durante gli spostamenti, mentre protegge i dati dentro e fuori l'ufficio.

- Processore Intel® Core™ i7 vPro™
- Windows 10 Pro
- Massima sicurezza con il sensore palm vein opzionale
- Notebook sottile, 33,8 cm (13,3 pollici) con display WQHD e opzione touch, con un peso di soli 1,37 kg
- Modular bay per drive ottico o seconda batteria



Schermate simulate, soggette a modifica. App Windows Store vendute separatamente. La disponibilità di app e l'esperienza possono variare in base al mercato.

workplace.it.fujitsu.com

© Copyright 2015 Fujitsu Technology Solutions. Fujitsu, il logo Fujitsu e i marchi Fujitsu sono marchi di fabbrica o marchi registrati di Fujitsu Limited in Giappone e in altri paesi. Altri nomi di società, prodotti e servizi possono essere marchi di fabbrica o marchi registrati dei rispettivi proprietari e il loro uso da parte di terzi per scopi propri può violare i diritti di detti proprietari. I dati tecnici sono soggetti a modifica e la consegna è soggetta a disponibilità. Si esclude qualsiasi responsabilità sulla completezza, l'attualità o la correttezza di dati e illustrazioni.

Viene presentato il prodotto pre-rilascio, soggetto a modifica.

Le app vengono vendute separatamente. Offerta di aggiornamento a Windows 10 valida per dispositivi Windows 7 e Windows 8.1 qualificati (compresi i dispositivi già in possesso) per un anno dalla disponibilità dell'aggiornamento a Windows 10.

Per maggiori informazioni visita la pagina windows.com/windows10upgrade.



Windows 10 Pro