STORMSHIELD

CONFORMITÀ ALLE NORME IN MATERIA DI SICUREZZA INFORMATICA PER AZIENDE DEL SETTORE DEI TRASPORTI

Per l'industria dei trasporti, assicurare la disponibilità operativa dei sistemi è un'esigenza imprescindibile e gli attacchi informatici possono pertanto arrecare danni fisici alle persone e all'ambiente. I rischi alle persone includono incidenti, deragliamenti, perdita di controllo di navi portacontainer all'ingresso in porto, incendi o avvelenamento da monossido di carbonio nei tunnel dovuto a perdita di ventilazione. Un comune esempio di rischio ambientale è invece rappresentato dalle perdite di petrolio nei mari con conseguenti effetti devastanti sulla fauna marina.

> NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA

> REQUISITI OPZIONALI DI CONFORMITÀ

> NORMATIVE LOCALI

> PER OGNI PROBLEMA C'È UNA SOLUZIONE STORMSHIELD

> LA CONFORMITÀ NON BASTA

> NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA

Le aziende del settore dei trasporti hanno l'obbligo di ottemperare alle seguenti normative europee in materia di sicurezza informatica:

Regolamento generale sulla protezione dei dati (GDPR)

Il GDPR è un regolamento europeo introdotto con il fine di armonizzare le norme in materia di riservatezza in vigore nei Paesi europei, nonché per tutelare le informazioni personali dei cittadini e rivoluzionare l'approccio adottato dalle aziende sul fronte della riservatezza dei dati. Tale regolamento introduce nuove limitazioni e nuovi requisiti che i Responsabili dei Sistemi informativi, i CIO e CISO sono tenuti a osservare.

I requisiti includono, tra gli altri, il principio della "Data protection by default", secondo cui la tutela dei dati personali deve avvenire per impostazione predefinita nell'ambito di servizi e sistemi. I prodotti Stormshield aiutano le organizzazioni a conformarsi a tali requisiti incrementando la resilienza delle rispettive infrastrutture informatiche. Stormshield Data Security mette a disposizione anche funzioni di crittografia dei dati, che il GDPR identifica come una misura tecnica adeguata a garantire un livello di protezione commisurato al rischio.

Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS)

La Direttiva NIS, ovvero la prima normativa europea in materia di sicurezza informatica, intende incrementare il livello complessivo di protezione all'interno dell'Unione europea e dovrà essere recepita negli ordinamenti giuridici degli stati membri. Ai sensi della direttiva NIS, ogni Paese è tenuto a designare Operatori di Servizi Essenziali (OES) in settori quali energia, trasporti, acqua potabile, infrastrutture del mercato bancario e finanziario, sanità e infrastrutture digitali. Gli OES designati avranno l'obbligo di conformarsi ai requisiti della direttiva.

Stormshield mette a disposizione prodotti certificati e affidabili per consentire agli OES di implementare soluzioni di sicurezza informatica capaci di potenziare il livello di protezione dei sistemi informativi essenziali. Ad esempio, Stormshield Network Security è in grado di isolare le aree di rete, garantire la sicurezza degli accessi da remoto, consentire l'autenticazione degli utenti e gestire le vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

> **NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA**

Payment Card Industry Data Security Standard (PCI-DSS)

Il PCI-DSS raggruppa una serie di norme di sicurezza delle informazioni applicabili alle aziende che raccolgono pagamenti mediante carte di credito emesse dalle principali società emittenti. L'osservanza di tali norme è obbligatoria per qualsiasi commerciante, istituzione finanziaria o altra persona giuridica che si fa carico dell'archiviazione, trattamento o trasmissione dei dati dei titolari di carte di pagamento. Le norme includono disposizioni in materia di sicurezza della rete, crittografia dei dati, gestione delle vulnerabilità e controllo efficace degli accessi.

I prodotti Stormshield permettono alle aziende di assicurare la conformità con molti dei principali requisiti PCI-DSS. Ad esempio, Stormshield Network Security (SNS) è in grado di isolare aree di rete e proteggere il traffico in uscita mediante crittografia, nonché gestire le vulnerabilità e l'autenticazione degli utenti. Stormshield Data Security (SDS) consente di crittografare i dati dei titolari di carta per garantirne l'integrità e la riservatezza. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus, rafforza la protezione della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

Direttiva relativa al riutilizzo dell'informazione del settore pubblico (PSI)

La Direttiva PSI introduce un quadro legislativo comune che incoraggia gli stati membri dell'UE a massimizzare il potenziale dell'informazione del settore pubblico rendendo possibile il riutilizzo della stessa. La PSI si applica a tutte le informazioni generate, raccolte o acquistate dagli enti pubblici. La Direttiva PSI, recepita nei vari ordinamenti giuridici nazionali, costituisce la base della politica di Open Data dell'Unione europea. Tutti gli enti che gestiscono informazioni a carattere pubblico o generano dati a partire da progetti di ricerca finanziati con fondi pubblici hanno l'obbligo di fornire l'accesso a tali informazioni, fatte salve limitazioni specifiche.

I prodotti Stormshield possono aiutare le organizzazioni a conformarsi ai requisiti della Direttiva PSI. In particolare, Stormshield Network Security (SNS) rende possibile la micro-segmentazione della rete per consentire l'isolamento dell'area di archiviazione dei dati pubblici. Inoltre, grazie alla gestione intuitiva delle politiche di protezione, SNS facilita l'identificazione delle aree di rete, la gestione degli accessi a livello di utente o di gruppo e l'introduzione di vincoli temporali.

> **NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA**

IEC 62443

La norma ISA-99/IEC 62443, creata dall'International Society of Automation, è lo standard globale per i sistemi di controllo industriali (ICS) e persegue il fine di contrastare il numero crescete di minacce informatiche. La norma permette alle organizzazioni di migliorare la protezione e la sicurezza digitale dei rispettivi processi e sistemi di controllo, quali DCS, PLC o SCADA. Deriva dalla famiglia di norme ISO/IEC 27000 ed è stata interamente adattato per consentirne l'applicazione negli ambienti dei sistemi di controllo industriali.

Il potenziamento della sicurezza informatica è un obiettivo multistrato che include governance, politiche di sicurezza e procedure organizzative. In un tale contesto, l'elevata affidabilità delle soluzioni Stormshield con certificazione "UE-Riservato" può aiutare le aziende a tutelarsi dall'azione delle minacce informatiche.

Ad esempio, Stormshield Network Security (SNS) è in grado di isolare le aree di rete, controllare i programmi PLC e consentire l'accesso sicuro da remoto finalizzato a interventi di manutenzione. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

Cybersecurity Act

Il regolamento europeo Cybersecurity Act rappresenta una riposta alla crescente minaccia di attacchi informatici, rafforzando le prerogative dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e dotandosi di un sistema europeo di certificazione in materia di cybersecurity. Questo sistema europeo di certificazione punta a rafforzare la sicurezza dei prodotti connessi, dei dispositivi dell'Internet delle cose e delle infrastrutture critiche tramite appositi certificati. Si tratta dunque di una certificazione di prodotti, processi e servizi che sarà valida in tutti gli Stati membri. I 3 livelli individuati ("di base", "sostanziale" ed "elevato") consentiranno agli utenti di stabilire il livello di affidabilità della sicurezza e garantiranno che gli elementi di sicurezza siano stati verificati in modo indipendente.

I prodotti Stormshield hanno già raggiunto il livello "Qualifica Standard" previsto in Francia dall'ANSSI (Agenzia nazionale per la sicurezza dei sistemi informativi). Sapendo che il livello «elevato» del sistema europeo corrisponde al livello "Qualifica Base" dell'ANSSI (che è inferiore al livello "Qualifica Standard"), i prodotti Stormshield sono dunque già conformi alle aspettative dell'ENISA in materia di cybersecurity.

Desideri saperne di più? Nessun problema!

> REQUISITI OPZIONALI DI CONFORMITÀ

Le aziende del settore dei trasporti che desiderino migliorare i propri livelli di sicurezza informatica dovrebbero adeguarsi anche agli standard seguenti, sebbene la conformità a questi non rappresenti un requisito normativo.

Common Criteria / Evaluation Assurance Level (EAL3+, EAL4+ ecc.)

"Common Criteria for Information Technology Security Evaluation" è una norma internazionale (ISO/IEC 15408) per la certificazione della sicurezza informatica. Serve ad assicurare che il processo di definizione delle specifiche, implementazione e valutazione delle soluzioni per la sicurezza informatica sia condotto in modo rigoroso, standardizzato e ripetibile, nonché a un livello commisurato al contesto di applicazione previsto. Ai sensi della norma, il "livello di garanzia della valutazione" attribuito (EAL3+, EAL4+ ecc.) indica l'accuratezza dei test a cui è stato sottoposto il prodotto in esame (ad es. un firewall). Questa certificazione è riconosciuta in 30 Paesi del mondo in Europa, Nord America, Asia e Medio Oriente.

I prodotti Stormshield non sono solo certificati ai sensi delle norme "Common Criteria", ma hanno raggiunto il livello più alto di "Qualifica Standard" rilasciato dall'ente francese ANSSI (Agenzia Nazionale per la Sicurezza dei Sistemi Informativi). Per conseguire tale status, i prodotti devono:

- Ottenere una certificazione di alto livello in base a un obiettivo di sicurezza stabilito e validato dall'ANSSI;
- Superare ulteriori procedure di valutazione svolte dall'ANSSI, inclusa un'analisi del codice sorgente.

Notare che la "Qualifica Standard" rappresenta un prerequisito per il rilascio delle denominazioni "NATO-Riservato" o "UE-Riservato" richieste per la gestione di informazioni classificate.

Standard ISO/IEC 27000 Tecnologie dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni

La serie ISO/IEC 27000 è una famiglia di norme in materia di sicurezza delle informazioni che fornisce un framework globalmente riconosciuto per una gestione efficace della sicurezza delle risorse informative. Caratterizzata da un ambito di applicazione deliberatamente ampio, questa serie di norme si applica ad aziende di qualsiasi dimensione e settore.

Il Sistema di gestione della sicurezza delle informazioni (ISMS) fornisce un approccio sistematico alla protezione di infrastrutture sensibili. In considerazione del carattere dinamico del rischio e delle misure di protezione richieste, l'ISMS incorpora feedback e miglioramenti costanti per reagire ai cambiamenti che interessano le minacce, le vulnerabilità o l'impatto di eventi imprevisti.

I prodotti Stormshield sono ideati per garantire la protezione delle infrastrutture sensibili. Il formato di log standard permette alle aziende di centralizzare tutte le informazioni, favorendo l'identificazione di trend e potenziali vulnerabilità. L'interfaccia grafica estremamente intuitiva facilita inoltre l'implementazione di miglioramenti da parte degli utenti.

> NORMATIVE LOCALI

FRANCIA

Legge di Programmazione Militare (LPM)

La Legge di Programmazione Militare (LPM) definisce l'orientamento della politica di difesa francese. A seguito dell'incremento di attacchi informatici condotti da hacker, terroristi e persino governi nazionali, garantire la resilienza dei sistemi informativi degli Operatori di Vitale Importanza (OIV) rappresenta un intento chiaramente stabilito nella LPM. La normativa affronta anche il tema della sicurezza informatica ed elenca gli OIV ripartiti in 12 settori di attività, tra cui il settore dei trasporti.

I prodotti Stormshield hanno ottenuto la certificazione dell'ANSSI (Agenzia Nazionale per la Sicurezza dei Sistemi Informativi) e favoriscono l'implementazione, da parte degli OIV, di soluzioni di sicurezza che consentono di incrementare il livello di protezione dei sistemi informatici critici. A titolo di esempio, Stormshield Network Security permette la segmentazione delle reti, la protezione degli accessi da remoto, l'autenticazione degli utenti e la gestione delle vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus, introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

Best practice ANSSI

L'Agenzia Nazionale per la Sicurezza dei Sistemi Informativi (ANSSI) riveste un ruolo chiave sul fronte della sicurezza informatica in Francia e si occupa inoltre di stilare periodicamente una serie di best practice. Non si tratta propriamente di "regolamenti", quanto piuttosto di linee guida finalizzate a supportare il processo decisionale per la selezione dei fornitori e delle soluzioni di sicurezza informatica, nonché per favorire l'implementazione delle medesime. Le best practice si concentrano su temi quali crittografia, sicurezza delle postazioni di lavoro e reti, proponendo risorse utili e approfondite.

> NORMATIVE LOCALI

GERMANIA

IT-Grundschutz

L'IT-Grundschutz è un insieme di norme elaborato dall'Ufficio Federale per la Sicurezza Informatica (Bundesamt für Sicherheit in der Informationstechnik, BSI) con il fine di soddisfare i requisiti corrispondenti a un livello di protezione adeguato per i dati e le informazioni. Ogni anno, a febbraio, viene pubblicato il IT-Grundschutz-Kompendium, il quale illustra i pericoli e i requisiti di sicurezza relativi a un tema di sicurezza informatica.

Ufficio Federale per la Sicurezza Informatica (BSI)

Le norme BSI sono una componente fondamentale della metodologia IT-Grundschutz. Gli attuali standard BSI sono i seguenti:

- 200-1 (Requisiti generali per sistemi di gestione della sicurezza delle informazioni)
- 200-2 (Fondamenti per lo sviluppo di una gestione efficace della sicurezza delle informazioni)
- 200-3 (Tutte le operazioni associate ai rischi nell'implementazione delle misure di sicurezza informatica di base)

Legge sulla sicurezza informatica (IT-Sicherheitsgesetz) e Legge BSI (BSI-Gesetz)

La Legge sulla sicurezza informatica stabilisce che gli operatori di servizi/infrastrutture critiche nel settore dei trasporti hanno l'obbligo di conformarsi a un livello minimo di protezione delle informazioni, segnalando eventuali interruzioni significative al BIS. In riferimento al concetto di "livello minimo di protezione", il paragrafo 8a del BSI-Gesetz è stato reso esecutivo mediante la Legge sulla sicurezza informatica, la quale definisce il "livello minimo" in termini astratti. Il 2016 ha visto inoltre l'introduzione del BSI-Kritisverordnung, il quale dettaglia i servizi critici che saranno tutelati ai sensi della Legge sulla sicurezza informatica. Tale ordinanza copre anche il settore dei trasporti.

Stormshield mette a disposizione prodotti certificati e affidabili per l'implementazione di soluzioni di sicurezza informatica capaci di potenziare il livello di protezione dei sistemi. Ad esempio, Stormshield Network Security è in grado di isolare le aree di rete, garantire la sicurezza degli accessi da remoto, consentire l'autenticazione degli utenti e gestire le vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing". Stormshield Data Security aiuta infine a prevenire le fughe di informazioni attraverso la cifratura di informazioni sensibili.

> NORMATIVE LOCALI

ITALIA

Decreto legislativo del 18 maggio 2018, n. 65 (Attuazione della direttiva (UE) 2016/1148)

Il Decreto introduce misure tese a garantire la tutela dei dati personali a livello nazionale, ivi compresi: la costituzione del CSIRT (noto anche con la denominazione CIRT); gli obblighi a carico dei cosiddetti "operatori di servizi essenziali" e dei fornitori di servizi digitali relativamente alle procedure per rispondere alle violazioni di sicurezza; i principi di cooperazione internazionale su questioni attinenti alla sicurezza; e l'adozione di una strategia nazionale di sicurezza informatica.

Stormshield mette a disposizione prodotti certificati e affidabili per consentire agli OES di implementare soluzioni di sicurezza informatica capaci di potenziare il livello di protezione dei sistemi informativi essenziali. Ad esempio, Stormshield Network Security è in grado di isolare le aree di rete, garantire la sicurezza degli accessi da remoto, consentire l'autenticazione degli utenti e gestire le vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

D.P.C.M. 17 febbraio 2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali - Decreto Gentiloni)

La Direttiva introduce gli organismi istituzionali incaricati della protezione cibernetica e della sicurezza informatica nazionali, disciplinando altresì gli obblighi e le responsabilità facenti carico a ciascun ente (CISR, CISR Tecnico, ruolo del DIS e linee guida applicabili, Nucleo per la sicurezza cibernetica e relative responsabilità). La Direttiva introduce inoltre misure applicabili agli "operatori di servizi essenziali" e ai fornitori di servizi di comunicazione.

D.P.C.M. 27 gennaio 2014 (Strategia nazionale per la sicurezza cibernetica - QSN)

La Strategia nazionale per la sicurezza cibernetica intende assicurare l'efficienza e l'interoperabilità delle risorse finalizzate alla difesa comune, al fine di incorporare nel processo di pianificazione della difesa in ambito NATO e nella dottrina militare un'efficace postura contro attacchi cibernetici.

Stormshield Network Security ha ricevuto la certificazione "UE-Riservato". Ciò significa che questi prodotti possono essere adoperati in contesti sensibili al fine di assicurare la trasmissione sicura di informazioni classificate, aiutando a garantire l'interoperabilità internazionale con le istituzioni UE.

> NORMATIVE LOCALI

SPAGNA

Legge PIC (Protezione delle infrastrutture critiche)

La Legge sulla protezione delle infrastrutture critiche (Ley PIC 8/2011) è integrata dal decreto reale 704/2011. La norma persegue principalmente i due obiettivi seguenti: classificare le infrastrutture responsabili dell'erogazione di servizi essenziali alla società, e ideare un piano di misure di prevenzione e protezione efficaci contro potenziali minacce alle suddette infrastrutture, sia dal punto di vista della sicurezza fisica che in termini di protezione delle tecnologie dell'informazione e della comunicazione.

Stormshield mette a disposizione prodotti certificati e affidabili per consentire alle infrastrutture critiche di implementare soluzioni di sicurezza informatica capaci di potenziare il livello di protezione dei sistemi informativi essenziali. Ad esempio, Stormshield Network Security è in grado di isolare le aree di rete, garantire la sicurezza degli accessi da remoto, consentire l'autenticazione degli utenti e gestire le vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

> PER OGNI PROBLEMA C'È UNA SOLUZIONE STORMSHIELD.

Prodotti e soluzioni Stormshield per il settore dei trasporti

> LA CONFORMITÀ NON BASTA

L'elevatissimo numero di norme e regolamenti è diventato un problema realmente difficile da gestire per le organizzazioni. La presente guida è stata creata per orientarsi tra le diverse normative applicabili ai vari settori industriali.
Ma la conformità non è tutto. Le aziende devono soprattutto imparare a individuare e gestire efficacemente i rischi a cui sono esposte se intendono realmente garantire la sicurezza delle informazioni.

Crediti fotografici: ShutterStock©, aressy.com