WISER

Wide-Impact cyber SEcurity Risk framework

Guida essenziale alla direttiva sulla sicurezza delle reti e dei sistemi informativi

Luglio 2016

www.cyberwiser.eu | info@cyberwiser.eu | @cyberwiser

WISER è un progetto di Innovation Action finanziato nell'ambito del programma Horizon 2020. Lo scopo del progetto è quello di sviluppare un frame work di gestione del rischio informatico in grado di valutare, monitorare e mitigare i rischi cyber.

WISER sta lanciando sul mercato una suite di servizi per la cyber security rivolti a piccole e medie imprese, infrastrutture critiche e sistemi informatici complessi.

CyberWISER Light è un servizio online gratuito di cyber risk assessment che comprende le più efficaci best practice nell'ambito della cyber security: dalla valutazione periodica sui rischi di sicurezza interni all'azienda, allo svolgimento di continui Vulnerability Test per valutare la sicurezza dell'azienda tramite simulazione di minacce esterne.

Nuovi servizi in arrivo a fine 2016

CyberWISER Essential: una soluzione avanzata di gestione del rischio per piccole e medie imprese.

CyberWISER Plus: una piattaforma di Risk Management-as-a-Service (RMPaaS) per infrastrutture o sistemi informatici complessi e che richiedono l'attuazione di controlli speciali e consentono la valutazione del livello di rischio a cui le Aziende sono esposte, oltre che la definizione di un adeguato piano di mitigazione dei cyber risk.

Disclaimer

Lo scopo di questa guida è quello di sensibilizzare settore pubblico e privato sull'adozione della direttiva NIS.
Tutte le organizzazioni interessate alla direttiva sono invitate a leggere il relativo documento ufficiale su Eur-Lex a questo link: http://ow.ly/pWO4302Gs10

Guida essenziale alla direttiva sulla sicurezza delle reti e dei sistemi informativi

La direttiva sulla sicurezza delle reti e dei sistemi informativi ('Direttiva NIS)è il primo esempio di regolamentazione di Cyber Security a livello Europeo.

La Direttiva NIS entrerà in vigore a partire da **Agosto 2016**. Gli stati membri avranno a disposizione **21 mesi** per adottare le necessarie misure di implementazione a livello di legislazione nazionale e 6 mesi supplementari per identificare gli operatori operanti nelle infrastrutture critiche nazionali.

L'obiettivo della direttiva è quello di raggiungere un più elevato livello di sicurezza dei sistemi delle reti e dell'informazione all'interno dell'UE tramite:

» Il miglioramento delle capacità di sicurezza informatica a livello nazionale.
» L'incremento di cooperazione tra i vari stati dell'Unione Europea
» Rendere obbligatoria la gestione dei rischi e degli incidenti per gli operatori di servizi essenziali e fornitori di servizi digitali.

1. . Le azioni degli Stati membri per aumentare e migliorare le capacità di sicurezza informatica a livello nazionale

Ogni Stato membro dovrà adottare una strategia nazionale sulla sicurezza dei sistemi di rete e di informazioni che definisca obiettivi strategici ed adeguate politiche e misure di regolamentazione. La strategia dovrebbe includere:

» Gli obiettivi strategici, le priorità e il quadro di governance.
» L' individuazione di misure in materia di preparazione, risposta e recupero.
» I metodi di cooperazione tra il settore pubblico e privato.
» La sensibilizzazione, la formazione e l'istruzione sul tema della sicurezza informatica

» I piani di ricerca e sviluppo per l'implementazione della Direttiva NIS
» I piani di valutazione del rischio informatico
» L' elenco degli attori coinvolti nella attuazione della strategia

Gli Stati membri designeranno una o più autorità nazionali competenti per la direttiva NIS, che ne controllino l'applicazione a livello nazionale.

Gli Stati membri dovranno inoltre designare un singolo punto di contatto, che eserciterà una funzione di collegamento per assicurare la corretta cooperazione con le autorità competenti degli altri Stati membri e con gli strumenti e le iniziative di cooperazione creati dalla direttiva stessa.

Gli Stati membri dovranno designare uno o più **Computer Security Incident Response Team** (CSIRT). I vari CSIRTs saranno responsabili di:

» Monitorare gli incidenti informatici a livello nazionale
» Fornire tempestivamente allarmi, avvisi ed annunci ai maggiori stakeholders con lo scopo di diffondere informazioni su rischi ed incidenti
» Fornire risposte tempestive ai vari incidenti
» Fornire analisi dinamiche dei rischi e degli incidenti e contribuire all'aumento della
» Partecipare alla rete del CSIRT nazionali (rete CSIRTs)

2. Member State actions to increase EU-level co-operation

La Direttiva NIS stabilisce la creazione di un **Gruppo di Cooperazione**, per sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri.

La Direttiva stabilisce anche la creazione di una rete dei CSIRT nazionali, al fine di contribuire allo sviluppo di una cultura della sicurezza e per promuovere una cooperazione operativa rapida ed efficace tra gli Stati membri.

Di cosa si occuperà il Gruppo di Cooperazione?

Il Gruppo di Cooperazione comprenderà rappresentanti degli Stati membri, la Commissione Europea (che avrà il ruolo di segretariato) e l'ENISA (l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione).

Il Gruppo di Cooperazione lavorerà sulla base di programmi di lavoro biennali, in quattro diverse aree:

Pianificazione:

» Stabilire un programma di lavoro di 18 mesi dopo l'entrata in vigore (cioè febbraio 2018).
» Preparare un programma di lavoro ogni due anni.

Guida:

» Fornire una fornire una guida per la rete dei CSIRTs
» Assistere gi Stati membri nello sviluppo della NIS
» Sostenere gli Stati membri nell'identificazione di operatori di servizi essenziali
» Discutere pratiche di notifica incidente
» Discutere standard
» Impegnarsi con le istituzioni e gli organi dell'UE
» Valutare le strategie nazionali e NIS CSIRTs (su base volontaria)
» Condividere le informazioni e le best practices in materia di:
» Rischi
» Incidenti
» Sensibilizzazione
» Formazione
» R & S

Seganalazione:

Fornire una valutazione complessiva delle esperienze acquisite tramite la cooperazione. La relazione sarà redatta ogni anno e mezzo ed inviata alla Commissione come contributo al riesame del funzionamento della direttiva.

Di cosa si occuperà la rete di CSIRTs?

La rete di CSIRTs sarà composta da rappresentanti degli CSIRTs degli Stati membri e di CERT-EU (la squadra di pronto intervento informatico per le istituzioni, agenzie e organismi Europei). La Commissione Europea parteciperà alla rete CSIRTs in qualità di osservatore. ENISA ricoprirà le funzioni di segreteria e sosterrà attivamente la cooperazione tra i CSIRTs.

La rete CSIRTs avrà i seguenti compiti:

» Condividere e promuovere informazioni sui servizi dei CSIRTs, le loro operazioni e attività, anche di cooperazione.
» Condividere e discutere le informazioni relative agli incidenti (su richiesta e volontario).

» Identificare una risposta efficace e coordinata ad un incidente (su richiesta e volontario).
» Aiutare nella gestione degli incidenti transnazionali (volontaria).
» Esplorare ulteriori forme di cooperazione operativa.
» Informare il Gruppo di Cooperazione delle sue attività e la richiesta di orientamento.
» Discutere e condividere esperienze emerse dall' esercizio della Direttiva NIS.
» Discutere problematiche relative ad un singolo CSIRT (su richiesta).
» Emanare linee guida sulle attività di cooperazione operativa

Due anni dopo l'entrata in vigore della direttiva NIS, e ogni 18 mesi successivi, la Rete CSIRTs produrrà una relazione per valutare l'esperienza acquisita con la cooperazione operativa, ivi comprese le conclusioni e le raccomandazioni emerse. La relazione sarà inviata alla Commissione come contributo al riesame del funzionamento della direttiva.

Obblighi legati alla gestione del rischio e alle notifiche degli incidenti per gli operatori di servizi essenziali e fornitori di servizi digitali.

Cosa sono gli operatori di servizi essenziali e cosa saranno tenuti a fare?

Gli operatori di servizi essenziali sono aziende private o enti pubblici con un ruolo importante per la società e l'economia. Ai sensi della direttiva NIS, gli operatori di servizi essenziali dovranno adottare misure di sicurezza appropriate e dovranno notificare gravi incidenti all'autorità nazionale competente. Le misure di sicurezza comprendono:

» Prevenzione del rischio: Adottare misure tecniche ed organizzative che siano adeguate e proporzionate al rischio in questione
» Garantire la sicurezza dei sistemi di rete e di informazione: Le misure devono garantire un livello di sicurezza dei sistemi e delle reti adeguati ai rischi in questione
» Gestione degli incidenti: Le misure dovranno prevenire e ridurre al minimo l'impatto degli incidenti sui sistemi informatici utilizzati per fornire i servizi.

In che modo uno Stato membro identifica gli operatori di servizi essenziali?

Ogni Stato membro dovrà identificare le entità che devono prendere opportune misure di sicurezza e notificare gli incidenti rilevanti tramite l'applicazione di questi criteri:

» L'entità fornisce un servizio che è essenziale per il mantenimento delle attività economiche / sociali critiche
» La fornitura di tali servizi dipende da sistemi di rete e di informazione

» Un incidente di sicurezza avrebbe effetti dirompenti e significativi sulla prestazione dei servizi essenziali

Quali sono i settori coperti dalla Direttiva?

La direttiva coprirà gli operatori nei seguenti settori:

» Energia: elettricità, petrolio e gas.
» Trasporto: aereo, ferroviario, marittimo e stradale.
» Bancario: gli istituti di credito.
» Infrastrutture dei mercati finanziari: le sedi di negoziazione e le controparti centrali.
» Salute: ambienti sanitari.
» Acqua: fornitura di acqua potabile e distribuzione.
» Infrastruttura digitale: specificamente gli Internet Exchange point, i fornitori di servizi DNS e i registri TLD.

Che tipo di incidenti dovranno essere riportati dagli operatori di servizi essenziali?

» La Direttiva non stabilisce una soglia quantitativa in base alla quale uno specifico incidente debba essere segnalato all'autorità competente, tuttavia vengono definiti 3 parametri che dovrebbero essere presi in considerazione:
» Numero di utenti interessati
» Durata temporale dell'incidente
» Diffusione geografica dell'incidente

Questi parametri potranno essere ulteriormente specificati dalle linee guida adottate dalle singole autorità competenti in concomitanza con il Gruppo di Cooperazione.

Quali sono i fornitori di servizi digitali e cosa dovranno fare?

I fornitori di servizi digitali – mercati online, motori di ricerca e servizi di cloud computing – ad eccezione delle micro e piccole imprese digitali dovranno, oltre a garantire la sicurezza delle loro infrastrutture, notificare gli incidenti più rilevanti alle autorità nazionali competenti.

Le misure di sicurezza per i fornitori di servizi digitali comprendono:

» Prevenzione del rischio: Adottare misure tecniche ed organizzative che siano adeguate e proporzionate al rischio in questione
» Garantire la sicurezza dei sistemi di rete e di informazione: Le misure devono garantire un livello di sicurezza dei sistemi e delle reti adeguati ai rischi in questione

» Gestione degli incidenti: Le misure dovranno prevenire e ridurre al minimo l'impatto degli incidenti sui sistemi informatici utilizzati per fornire i servizi.

Le misure di sicurezza per i fornitori digitali dovrebbero tenere in considerazione anche altri fattori più specifici che saranno meglio definiti in una direttiva di implementazione della Commissione Europea:

» Sicurezza dei sistemi e impianti.
» Gestione degli incidenti.
» Gestione della continuità operativa.
» Monitoraggio, controllo e collaudo.
» La conformità con gli standard internazionali.

Che tipo di incidenti dovranno essere riportati dai fornitori di servizi digitali?

La Direttiva non stabilisce una soglia quantitativa in base alla quale uno specifico incidente debba essere segnalato all'autorità competente, tuttavia vengono definiti 5 parametri che dovrebbero essere presi in considerazione:

» Numero di utenti interessati
» Durata temporale dell'incidente
» Diffusione geografica dell'incidente
» L'estensione del disservizio
» L'impatto sulle attività economiche e sociali

Questi parametri saranno ulteriormente specificati dalla Commissione Europea mediante specifici atti esecutivi.

Quali fornitori di servizi digitali saranno tenuti ad adottare la NIS?

» Online marketplace
» Online search engine
» Cloud computing service

Tutte le entità che soddisfano questi requisiti saranno automaticamente soggetti agli obblighi di sicurezza e di notifica ai sensi della direttiva NIS. Micro e piccole imprese (come definite nella raccomandazione 2003/361/EC della Commissione) non rientrano nell'ambito di applicazione della direttiva.

Come verrà raggiunto un approccio armonico ed efficiente per i fornitori di servizi digitali?

La Commissione Europea adotterà atti di esecuzione per quanto riguarda i requisiti di sicurezza e gli obblighi di notifica dei fornitori di servizi

digitali entro un anno dall'adozione della direttiva. Gli Stati membri non saranno in grado di imporre ulteriori e più stringenti requisiti di sicurezza e di notifica ai fornitori. Inoltre, le autorità competenti saranno in grado di esercitare attività di vigilanza solo se provviste dell'effettiva evidenza che uno specifico fornitore non si è conformato agli obblighi derivanti dalla direttiva.

Useful links

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

http://ow.ly/pWO4302Gs10

Digital Single Market: cyber security

http://ow.ly/Pc9I302Gs5A

Fact Sheet on Cyber Security in EU

http://ow.ly/YkSJ302Gs83

EC Press Release on NIS Directive approval by EU Parliament

http://ow.ly/Z5Nk302Gsaf

Qual è la timeline per l'implementazione della Direttiva?

Agosto 2016

Entrata in vigore

6 mesi

Febbraio 2017

Inizio dei lavori del Gruppo di Cooperazione

12 mesi

Agosto 2017

Adozione dei requisiti di sicurezza e notifica per i fornitori di servizi digitali

18 mesi

Febbraio 2018

Il Gruppo di Cooperazione stabilisce il programma di lavoro

21 mesi

Maggio 2018

Recepimento nella legislazione nazionale

27 mesi

Novembre 2018

Gli Stati membri identificano gli operatori dei servizi essenziali

33 mesi

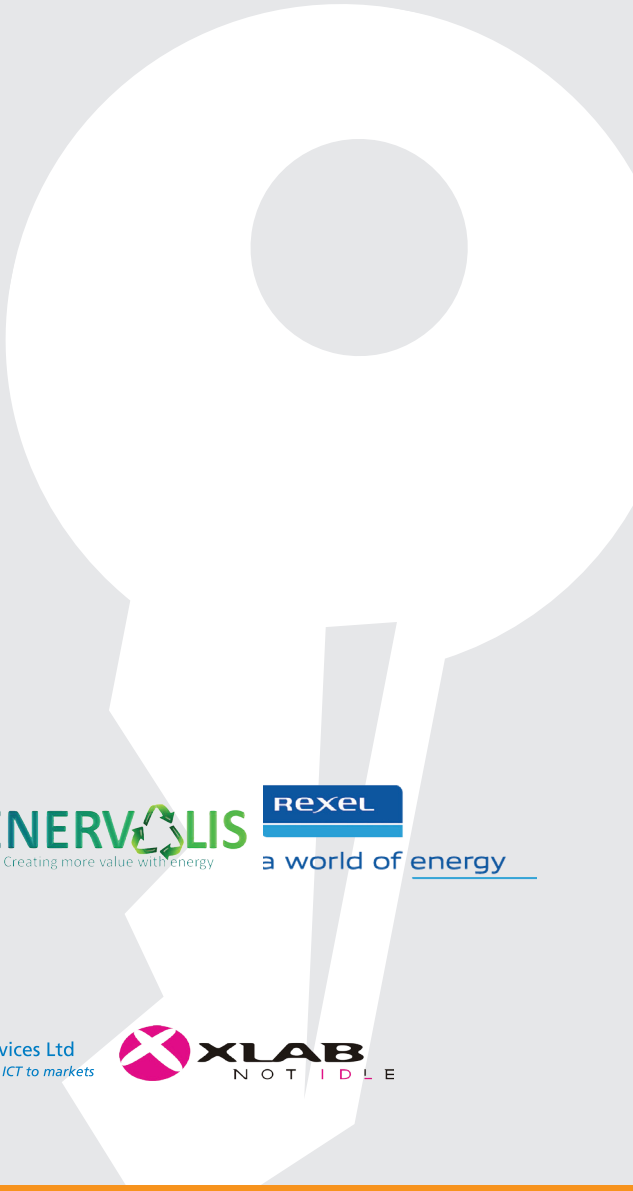
Maggio 2019

Prima relazione della Commissione Europea per valutare il lavoro degli Stati membri nell'identificazione degli operatori di servizi essenziali

57 mesi

Maggio 2021

La Commissione Europea valuta l'implementazione della Direttiva con particolare attenzione alla cooperazione strategica e operativa, e alle relazioni con i gestori dei servizi essenziali e con i fornitori di servizi digitali



Entra a far parte della community di WISER per avere accesso gratuito a CyberWISER Light, e scopri le ultime notizie e aggiornamenti sul mondo della cyber security.

Iscriviti alla newsletter:

Seguici su Twitter:

Connettiti su LinkedIn:

European Commission