

1. 290-192A5_02 - Network e information systems



FIASS
FORMAZIONE
INTERMEDIARI
ASSICURATIVI

Corso e-learning IVASS

Network & Information Systems

La NIS 2 e le opportunità del mondo delle assicurazioni

FORMAZIONE E-LEARNING AI SENSI DEL REG.IVASS VIGENTE

Video Lezione: **2/3** | Docente: **Laura Lucchi** | Durata Modulo: **un'ora circa** | CM: **290-192A5_02**

1.2 Come si identificano le vulnerabilità nella rete aziendale



Come si identificano le vulnerabilità nella rete aziendale

Identificare le vulnerabilità nella rete aziendale è un processo cruciale per garantire la sicurezza informatica. Le aziende possono adottare diverse metodologie e strumenti per rilevare e gestire queste vulnerabilità, vediamo alcune metodologie.

FIASS
FORMAZIONE
INTERMEDIARI
ASSICURATIVI

1.3 Vulnerability assessment

Vulnerability assessment

È un **processo sistematico** che mira a **identificare e classificare le vulnerabilità** nei sistemi informativi aziendali. Utilizza **strumenti di scansione** per analizzare server, applicazioni web, dispositivi di rete e database, evidenziando eventuali punti deboli e suggerendo soluzioni.

Effettuare un *Vulnerability Assessment* consente di **scoprire se la nostra aziende** o il sito Web **presentino vulnerabilità** che potrebbero mettere a rischio attacco informatico il prezioso patrimonio informativo. Ecco cos'è un VA, perché è utile e come effettuarlo.

Si utilizzano **Vulnerability Scanner**: strumenti come **Nessus** o **Open VAS** per eseguire scansioni approfondite dei sistemi e *generare report* sulle vulnerabilità identificate.



1.4 I SIEM

I SIEM

Security Information and Event Management (SIEM): Questi strumenti raccolgono e analizzano i dati di sicurezza in tempo reale, aiutando a identificare **comportamenti anomali** che potrebbero indicare una vulnerabilità o un attacco in corso.

Verificare le *configurazioni dei sistemi e dei dispositivi di rete* è fondamentale per identificare **configurazioni errate che potrebbero esporre l'organizzazione a rischi**. Questo include controlli su firewall, router e server.



1.5 Penetration Testing



Penetration Testing

Il Penetration test **simula attacchi reali** per identificare le vulnerabilità sfruttabili da un attaccante. A differenza del Vulnerability assessment, che si limita a scansionare i sistemi, il Penetration test **verifica attivamente come un attaccante** potrebbe compromettere la rete.



1.6 Network scanning

Network scanning

Le **tecniche di scansione della rete**, come la scansione delle porte e degli indirizzi IP, consentono di **mappare i dispositivi connessi alla rete e identificare eventuali porte aperte o servizi vulnerabili**. Queste scansioni possono essere *effettuate sia internamente che esternamente alla rete aziendale*.

Gli strumenti utilizzati a tal fine sono specifici per la scansione della rete, come **Nmap**, consentono di **mappare la rete aziendale e identificare i dispositivi attivi**, le porte aperte e i servizi in esecuzione.



1.7 Monitoraggio



Monitoraggio

Implementare **soluzioni di monitoraggio continuo** delle vulnerabilità permette di rilevare **in tempo reale** eventuali **nuove minacce o cambiamenti** nella sicurezza della rete. Questi strumenti possono eseguire **scansioni automatiche** e fornire **report aggiornati** sulle vulnerabilità.



1.8 Risoluzione

Risoluzione

Una volta che le vulnerabilità sono state classificate in ordine di priorità, i *team di sicurezza* possono **risolvere in uno dei tre modi seguenti**:

Correzione: risolvere completamente una vulnerabilità in modo che non possa più essere sfruttata, ad esempio **installando una patch che corregge un bug** del software o ritirando una risorsa vulnerabile. Molte piattaforme di gestione delle vulnerabilità forniscono strumenti di riparazione come la gestione delle patch per download e test automatici delle patch e la gestione della configurazione per affrontare configurazioni errate di rete e dispositivi da un dashboard o portale centralizzato.

Mitigazione: rendere una **vulnerabilità più difficile da sfruttare e ridurre l'impatto dello sfruttamento** senza rimuoverla completamente. Lasciare online un dispositivo vulnerabile ma segmentarlo dal resto della rete è un esempio di mitigazione. La mitigazione viene spesso eseguita quando una patch o altri mezzi di correzione non sono ancora disponibili.

Accettazione: scegliere di **non affrontare una vulnerabilità**. Le vulnerabilità con *punteggi di criticità bassi*, che è improbabile che vengano sfruttate o che causino danni significativi, vengono spesso accettate.



1.9 Accettazione del Rischio

Accettazione del Rischio

L'accettazione del rischio implica **riconoscere un rischio** e decidere di non intraprendere azioni attive per evitarlo, mitigarne l'impatto o trasferirlo. Questa scelta può essere sia **passiva che attiva**:

- **Accettazione Passiva:** non viene intrapresa alcuna azione per affrontare il rischio. Si accetta semplicemente che il rischio esista e si è pronti ad affrontarne le conseguenze se si materializza.
- **Accettazione Attiva:** anche se non si agisce per ridurre il rischio, si possono pianificare delle contromisure o piani di emergenza per affrontare eventuali eventi avversi quando si verificano.

L'accettazione è spesso una scelta praticabile **quando i costi per mitigare o trasferire un rischio superano i potenziali danni che quel rischio potrebbe causare**. È importante che le organizzazioni valutino attentamente la probabilità e l'impatto di un rischio prima di decidere di accettarlo.



1.10 Trasferimento del Rischio

Trasferimento del Rischio

Il **trasferimento del rischio** consiste nel **spostare la responsabilità di un rischio a un'altra parte**, solitamente attraverso **contratti o assicurazioni**. Questo metodo non riduce la probabilità che un evento rischioso si verifichi, ma **limita l'impatto finanziario o operativo su chi trasferisce il rischio**.

Ecco alcuni esempi comuni:

- **Assicurazioni:** un esempio classico è l'**assicurazione contro gli incidenti**, dove il rischio finanziario associato a un incidente viene trasferito alla compagnia assicurativa. In questo modo, l'organizzazione paga un premio per proteggersi da potenziali perdite economiche.
- **Outsourcing:** un altro modo di trasferire il rischio è **delegare certe attività a terzi con maggiore esperienza o capacità**. Ad esempio, un'azienda può esternalizzare la gestione della sicurezza informatica a specialisti esterni, riducendo così il proprio carico di responsabilità in caso di violazioni della sicurezza.



1.11 I punti essenziali di NIS2



I punti essenziali di NIS2

1. Analisi dei rischi e politiche di sicurezza dei sistemi informativi.
2. Gestione degli incidenti (prevenzione, individuazione e risposta).
3. Continuità operativa e gestione delle crisi.
4. Sicurezza della catena di approvvigionamento.
5. Sicurezza nell'acquisizione, sviluppo e manutenzione della rete.
6. Politiche e procedure (test e audit) e formazione.
7. Uso della crittografia, della cifratura e di soluzioni MIA.
8. Sicurezza delle risorse umane, controllo dell'accesso e gestione attivi.

1.12 Gestione degli Incidenti

Gestione degli Incidenti

Processo di Gestione degli Incidenti



Definizione di Procedure: le entità devono **stabilire procedure chiare per la rilevazione, gestione e risposta agli incidenti di sicurezza informatica**. Questo include l'**assegnazione di ruoli e responsabilità specifiche all'interno dell'organizzazione**.

Monitoraggio e Registrazione: è necessario **implementare sistemi di monitoraggio** per rilevare attività sospette e **registrare gli incidenti in modo dettagliato**, facilitando così la risposta e l'analisi successiva.



1.13 Definizione di procedure Incident Response

Definizione di procedure Incident Response

Per un'organizzazione che desidera essere **conforme alla direttiva NIS2**, è fondamentale implementare **procedure di Incident Response efficaci**. Queste procedure devono garantire una gestione sistematica degli incidenti di sicurezza informatica, dalla rilevazione alla risposta e alla comunicazione.

Ecco i principali passaggi da seguire:

1. Sviluppo di un Piano di Risposta agli Incidenti

Definizione del Piano: creare un **piano dettagliato** che delinei come l'organizzazione intende rilevare, segnalare e rispondere agli incidenti di sicurezza informatica. Questo piano **dove essere allineato con i requisiti della NIS2 riguardo alla segnalazione degli incidenti**.



1.14 Definizione di procedure Incident Response

Definizione di procedure Incident Response

2. Identificazione e Rilevazione degli Incidenti

Monitoraggio Continuo: implementare **sistemi di monitoraggio** per identificare attività sospette o anomalie nei sistemi informatici. Utilizzare strumenti di rilevamento delle intrusioni e altre tecnologie per garantire una **sorveglianza efficace**.

Formazione del Personale: assicurarsi che il **personale sia addestrato a riconoscere segnali di allerta e anomalie**, contribuendo così a una rilevazione precoce degli incidenti.



1.15 Definizione di procedure Incident Response

Definizione di procedure Incident Response

3. Segnalazione degli Incidenti

Tempistiche di Notifica: in caso di incidenti significativi, le **organizzazioni devono notificare le autorità competenti** (come il Computer Security Incident Response Team - CSIRT) **entro 24 ore** dall'identificazione dell'incidente. Un *rapporto dettagliato deve essere presentato entro 72 ore*.

Documentazione: mantenere **registrazioni accurate degli incidenti**, inclusi i dettagli su come è stato rilevato l'incidente, le misure adottate e gli impatti.



1.16 Modalità dell'obbligo di notifica degli incidenti



Modalità dell'obbligo di notifica degli incidenti

Le **Entità essenziali e importanti dovranno:**

1. **ENTRO 24 ORE** – inviare una pre notifica, per comunicare che i soggetti sono venuti a conoscenza dell'incidente significativo, inoltre **ENTRO 24 ORE** si dovrà effettuare la comunicazione dell'incidente a ACN.
2. **ENTRO 72 ORE** – inviare una notifica dell'avvenimento.
3. **UNA EVENTUALE RELAZIONE INTERMEDIA**, su richiesta di CSIRT Italia.
4. **ENTRO UN MESE DALLA TRASMISSIONE DELLA NOTIFICA** - una eventuale relazione finale.



1.17 Cosa si intende per «incidente»

Cosa si intende per «incidente»

QUASI INCIDENTE:

un *evento che avrebbe potuto compromettere* la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati ma che è stato efficacemente evitato o non si è verificato.

INCIDENTE:

un *evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi.*

INCIDENTE SU LARGA SCALA:

un *incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri.*



1.18 Definizione di procedure Incident Response

Definizione di procedure Incident Response

4. Risposta agli Incidenti

Attuazione delle Misure di Mitigazione: stabilire **procedure per affrontare gli incidenti, inclusa la quarantena dei sistemi compromessi e il ripristino dei servizi.** È essenziale avere un team dedicato che gestisca la risposta agli incidenti.

Comunicazione Interna ed Esterna: definire **protocolli di comunicazione** per informare i membri dell'organizzazione e le **parti interessate esterne** (clienti, partner) in merito all'incidente e alle misure adottate per affrontarlo.



1.19 Definizione di procedure Incident Response

Definizione di procedure Incident Response

5. Formazione Continua e Aggiornamento delle Procedure

Formazione Regolare: implementare **programmi di formazione continua** per il personale sulla gestione degli incidenti e sulla sicurezza informatica in generale.

Revisione Periodica del Piano: rivedere e **aggiornare regolarmente il piano di risposta agli incidenti** per adattarsi a *nuove minacce* e cambiamenti nel contesto operativo dell'organizzazione.



1.20 Fine

FIAss
FORMAZIONE
INTERMEDIARI
ASSICURATIVI

→

Fine

Seconda parte

💡 Per domande al docente usa il tasto **Help Desk** o scrivi a info@fiaass.it

💻 Se hai problemi di visualizzazione o salvataggio consulta il “**Modulo Guida ai Corsi FIAss**”

🕒