Titolo:

Sicurezza Informatica nella Provincia di Perugia

Sottotitolo:

- Adesione all'Accordo Quadro "Cybersecurity 2«
- Le politiche di sicurezza adottate dall’ente
- Recepimento della Direttiva NIS 2

Contesto e Obiettivi:

- Crescente minaccia degli attacchi informatici
- Necessità di aggiornare le politiche di sicurezza
- Obiettivo: rafforzare la resilienza informatica dell’Ente

Accordo quadro Cybersecurity 2

- A Settembre 2023 si è aderito all'accordo quadro Cybersecurity 2
- Acquisizione di Firewall NGFW (Next-Generation Firewall);
- Acquisizione di una Piattaforma antivirus;
- Acquisizione di Supporto specialistico per implementazione e gestione di nuovi sistemi di sicurezza.

Accordo quadro Cybersecurity 2

Componenti Tecnologiche Implementate Parte 1:

- **2 Firewall NGFW in alta affidabilità**;
- **Piattaforma antivirus per 500 PC e 40 server**;
- **Piattaforma SIEM** (Security Information and Event Management) che centralizza e analizza log e dati di sicurezza da diverse fonti (server, dispositivi di rete, firewall, ecc.) per rilevare minacce in tempo reale e supportare analisi, combina due funzioni principali:
  - la gestione e l'archiviazione a lungo termine dei dati (SIM);
  - monitoraggio in tempo reale e la correlazione degli eventi (SEM).

(gli approfondimenti tecnici saranno discussi più avanti)

Accordo quadro Cybersecurity 2

Componenti Tecnologiche Implementate Parte 2:

- **Implementazione di un sistema IDS** (Intrusion Detection System), strumento di sicurezza (Server Fisico) che monitora il traffico di rete per individuare e segnalare attività dannose o sospette generando allarmi per un possibile intervento per bloccare l'attacco;
- **Implementazione di un Servizio SOC (Security Operations Center) integrato con il Servizio SIEM** che monitora e protegge le risorse informatiche adibito alla prevenzione di minacce e cyberattacchi e impiegato anche per un pronto intervento (anche in maniera automatica) in caso di incidente.

(anche qui gli approfondimenti tecnici saranno discussi più avanti)

Accordo quadro Cybersecurity 2

Inoltre Il supporto specialistico è stato utilizzato anche per implementare i seguenti servizi:

- Approfondire le funzioni già incluse nel Server SIEM;
- Installazione ed integrazione di servizi e agenti per aumentare il dettaglio dei Log (Tecnologia Elastic);
- Data Analysis;
- Investigation;
- Threat Hunting (Ricerca delle Minacce);
- Identificazione Vulnerabilità e Attività di Remediaton;
- Alert Ranking and Management;
- Alert per minacce emergenti;
- Security Compliance (conformità alla sicurezza);
- Vulnerability Assessment (scoprire e correggere i punti deboli);
- Security Awareness (acquisire conoscenze e comportamenti sicuri).

Le politiche di sicurezza adottate dall’ente:

- Protocollo d’intesa per la prevenzione e il contrasto dei crimini informatici con la Polizia Postale;
- Costituzione del Comitato Cyber Security
- Politiche di sicurezza implementate a livello tecnico, di sistemi ed infrastrutture

Le politiche di sicurezza adottate dall’ente

Protocollo con la Polizia Postale:

- Firmato il 23/04/2024
- Collaborazione per prevenzione e contrasto crimini informatici
- Condivisione informazioni e gestione emergenze

Fasi propedeutiche alla Costituzione del Comitato Cyber Security – Parte 1

L’attività tecnica da attuare per garantire la sicurezza del sistema informativo dell’ente **doveva inoltre essere supportata da una serie di processi aziendali** che trovavano fondamento nel quadro normativo di riferimento (regolamenti, direttive e decreti attuativi che regolano la sicurezza dei sistemi informatici) e per supportare tale scopo, con determinazione dirigenziale del 03/05/2024, **sono stati acquisiti servizi aggiuntivi di Cyber Security**.

Le politiche di sicurezza adottate dall'ente

Fasi propedeutiche alla Costituzione del Comitato Cyber Security – Parte 2

I Servizi aggiuntivi di Cyber Security erano composti dalle seguenti macro-fasi:

- definizione delle norme di sicurezza applicabili;
- raccolta delle informazioni sullo stato di applicazione delle norme di riferimento;
- valutazione del GAP tra quanto previsto dalle norme e quanto applicato;
- definizione delle attività necessarie per la compliance (conformità) totale alle norme di riferimento individuate;
- identificazione delle aree che richiedono particolare attenzione in merito alle azioni da intraprendere;
- redazione della documentazione necessaria per la compliance (conformità), comprese procedure, policy di cybersecurity, regolamenti e manuali che poi saranno approvati e aggiornati periodicamente dal Comitato di Cyber Security;
- rilascio parere tecnico di fattibilità su specifici casi;

Costituzione del Comitato Cyber Security – Motivazioni

Al fine di garantire le necessarie attività di coordinamento degli interventi messi in campo dalla Provincia di Perugia per quanto attiene alla sicurezza informatica, si è ritenuto necessario costituire un Comitato di Gestione della Cybersecurity, composto da varie professionalità interne all’Ente, coerentemente con quanto previsto dalle disposizioni del DPR 13/06/2023, n. 81, nel quale è data facoltà all’amministrazione di adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici e dei dati.

Le politiche di sicurezza adottate dall’ente

In Sintesi:

- Comitato Cyber Security è stato costituito nell’anno 2024 ed integrato nel 2025;
- Composizione multidisciplinare;
- Coordinamento e governance della sicurezza.

Le politiche di sicurezza adottate dall’ente

Composizione multidisciplinare del Comitato

- Direttore Generale o suo delegato;
- DPO - Data Protection Officer;
- Dirigente Servizio Sistemi Informativi/Responsabile Transizione Digitale;
- I Responsabili dei vari uffici dei servizi informatici (Infrastrutture Digitali, Piattaforme Gestionali, Transizione al digitale);
- Supporto Tecnico-Informatico specialistico al Comitato

Le politiche di sicurezza adottate dall’ente

Ogni componente del comitato porta una competenza unica e una prospettiva critica per la gestione complessiva della cyber security.

Il comitato, per cercare di prevenire gli attacchi, opera con una chiara struttura di governance, con incontri regolari, e un flusso di comunicazione efficace per coordinare le attività e rispondere rapidamente a qualsiasi minaccia.

Il comitato si incontra regolarmente ogni 4 Mesi per discutere:

- Report di sicurezza che il SOC (Security Operations Center) - invia all’ente ogni 4 mesi e che si dividono in:
  - Report di Sicurezza dei servizi informatici e dei Server esposti a internet (External)
  - Report di Sicurezza dei PC interni all’ente (internal_endpoints)
  - Report di Sicurezza dei Server interni all’ente (internal_servers)
  - Vulnerability Assessment Report
- Come migliorare ed integrare le politiche di Cyber Sicurezza fin qui implementate con nuove tecniche, nuovi sistemi e nuovi protocolli di comunicazione;

Politiche di sicurezza implementate a livello tecnico, di sistemi ed infrastrutture – Parte 1

1. Nessun utilizzo di NAS o cartelle condivise nel data center on premise ma utilizzo di solo Google Drive per la condivisione di file e cartelle fra Aree e Servizi dell'ente;
2. Per ridurre i disservizi verso tale servizio è stata dedicata una Banda internet sul Firewall per appunto i servizi Google;
3. Posta elettronica in Cloud (Servizio Google G-Mail);
4. Utilizzo di una piattaforma per criptare i dati sensibili e condividerli;
5. Utilizzo di una piattaforma antivirus centralizzata con possibilità di creare bolle virtuali per monitorare il file scansionato e per eseguire tale file solo dentro la bolla virtuale per studiare il suo comportamento;
6. Disabilitazione USB sui PC o Allarme dall'agente antivirus quando vengono copiati dei dati su chiavetta USB;
7. n.2 Firewall di Nuova Generazione per un controllo puntale e filtraggio anche a livello di applicazione (livello 7 OSI);

Politiche di sicurezza implementate a livello tecnico, di sistemi ed infrastrutture – Parte 2

8. Implementazione di un Server WSUS per la gestione ed il deploy degli aggiornamenti di sicurezza dei Sistemi Operativi di PC e Server;

9. Implementazione di un Server SIEM con tecnologia Elsatic la per raccolta, gestione e analisi dei log da tutti i sistemi e server di rete;

10. Tutti i Server, PC, piattaforma antivirus, Piattaforma Google Workspace (Posta, condisione file e cartelle, calendario, ecc…) integrato con gli agenti Elastic per la raccolta dei Log in SIEM;

11. Un sistema IDS (Intrusion Detection System) con sonda di rete dedicata, è un server fisico, posizionato nel punto strategico dell'infrastruttura per l'analisi del traffico (centro stella con porta in mirroring di tutto il traffico dell'ente) e che invia i Log in SIEM;

12. Utilizzo di un Supporto specialistico per l'analisi dei Log e per la creazione di Report sulle falle di sicurezza di PC e server interni ed esterni;

13. Ricezione di Mail redatte dal supporto specialistico in cui riceviamo le falle di vulnerabilità sia hardware che software e con le azione da eseguire per la loro risoluzione;

Politiche di sicurezza implementate a livello tecnico, di sistemi ed infrastrutture – Parte 3

14. Ricezione di Mail e PEC dalla Polizia Postale in cui vengono inviati gli ultimi Alert e Report sulle vulnerabilità riscontrate e note dei sistemi e software a livello nazionale;

15. Stretta collaborazione sempre con la polizia postale per la formazione e del Personale e nella gestione della prevenzione e risoluzione di possibili incidenti informatici attraverso il Protocollo d'intesa sopra citato;

16. Smart working: Passaggio da utilizzo di VPN con doppia autenticazione (già sicura) alla nuova tecnologia ZTNA (Zero Trust Network Access, accesso remoto sicuro alle applicazioni aziendali) sempre con doppia autenticazione (ZTNA tratta ogni utente e dispositivo individualmente in modo che siano messe a disposizione solo le risorse a cui esso e il dispositivo possono accedere. Invece di permettere agli utenti la completa libertà di movimento nella rete come la VPN, vengono stabiliti tunnel individuali tra l'utente e il gateway) specifico per l'applicazione verso la quale sono autorizzati ad accedere;

17. Autenticazione con doppio fattore di tutti i servizi (Posta, Drive, ZTNA, VPN);

Politiche di sicurezza implementate a livello tecnico, di sistemi ed infrastrutture – Parte 4

18. Disabilitazione degli utenti come amministratore del computer e in caso di necessità, prima di un'installazione di un nuovo software, viene fatto l'inventario attraverso una piattaforma specifica del software presente prima e dopo l'installazione;

19. Utilizzo di una Piattaforma (Lansweeper) che gestisce le risorse IT automatizzando l'inventario di tutti i dispositivi hardware e software presenti in una rete, in ambienti fisici, virtuali e cloud;

20. Formazione continua del personale sulla Sicurezza Informatica con corsi on-line (CyberGuru) o in presenza con la Polizia Postale;

21. Backup di tipo BaaS – (Backup as a Service) con regolari Test di Restore e che produce dei Report di Test Restore in cui sono descritti i processi effettuati e viene verificata l'integrità e l'affidabilità del sistema di backup utilizzato.

Recepimento della Direttiva NIS 2

Direttiva NIS 2: obbligo non per tutti ma best practice da tenere in considerazione

- **Dal 16 ottobre 2024 è in vigore anche in Italia il d.lgs. 4 settembre 2024, n. 138**, che recepisce la Direttiva (UE) 2022/2555, conosciuta come NIS 2 (Network and Information Systems Directive)
- **la Direttiva Europea NIS 2** rappresenta un passo cruciale per aumentare la sicurezza dei sistemi informativi nei settori critici come energia, trasporti, sanità e infrastrutture digitali.
- **Il Regolamento (UE) 2024/2690**, pubblicato a luglio 2024, stabilisce i requisiti tecnici e metodologici per la gestione dei rischi di cybersicurezza e definisce cosa si intende per incidente significativo, applicandosi a settori come i fornitori di servizi di cloud computing, i mercati online e i prestatori di servizi fiduciari. In pratica, traduce la direttiva NIS 2 in norme specifiche per settori critici, chiedendo loro di adottare misure di sicurezza rigorose e di implementare procedure per la gestione e la notifica degli incidenti.

Recepimento della Direttiva NIS 2

Cosa cambia rispetto alla NIS 1

1. **Ampliamento dei soggetti coinvolti**. La NIS 2 estende il campo di applicazione a un numero maggiore di settori e aziende, rispetto alla precedente direttiva del 2016.
2. **Obblighi più precisi e vengono introdotti requisiti tecnici e organizzativi più dettagliati**, nonché un sistema sanzionatorio più severo.
3. **Responsabilità dei dirigenti**. Maggiore responsabilità diretta per il management aziendale in caso di mancata conformità.
4. **Supply chain**. Estensione degli obblighi anche alla catena di fornitura, imponendo controlli sui fornitori.
5. **Il REGOLAMENTO DELLA COMMISSIONE 2024/2690** stabilisce criteri oggettivi per la classificazione e la notifica degli incidenti significativi

Recepimento della Direttiva NIS 2

NIS 2 - Chi deve adeguarsi - La normativa distingue tra due categorie principali:

1. **Soggetti essenziali** (Energia, trasporti, sanità, banche, infrastrutture digitali, acqua e rifiuti, enti pubblici strategici) con più di 50 dipendenti o più di 10 mln di euro di fatturato.

2. **Soggetti importanti** (Cloud provider, data center, fornitori di servizi digitali, produttori hardware/software, logistica, settore spaziale, ecc.) con più di 50 dipendenti o più di 10 mln di euro di fatturato.

3. **Sono tenute a conformarsi tutte le aziende con almeno 50 dipendenti o un fatturato annuo superiore a 10 milioni di euro**. Tuttavia, anche aziende più piccole possono essere coinvolte se operano in settori critici o forniscono servizi essenziali a soggetti obbligati.

4. **La normativa si applica anche a pubbliche amministrazioni fino al livello locale**, Tutte le Pubbliche Amministrazioni centrali (e molte locali) sono ora soggette agli obblighi, indipendentemente dalle dimensioni.

5. **Sono inclusi gli organi costituzionali, la Presidenza del Consiglio dei Ministri, i Ministeri, le Agenzie fiscali, le Autorità amministrative indipendenti e gli enti locali (regioni, città metropolitane, comuni con più di 100.000 abitanti). Inoltre, sono interessate le aziende sanitarie locali (ASL) e altri enti pubblici rilevanti come istituti di ricerca, enti regolatori, enti che forniscono servizi culturali o assistenziali, e istituti zooprofilattici sperimentali.**

6. **L'obiettivo è rendere i sistemi informativi pubblici più resilienti, garantendo la continuità dei servizi essenziali e la protezione dei dati dei cittadini.**

NIS 2 - Principali novità e adempimenti per le PA

1. **Identificazione dei servizi critici.**
2. **Valutazione e gestione dei rischi.**
3. **Notifica degli incidenti.**
4. **Responsabilità e governance**
5. **Registrazione presso ACN (non ancora obbligatorio per la Provincia).**
6. **Collaborazione con ACN. Le PA devono collaborare attivamente con l'ACN per la gestione degli incidenti e per le attività di analisi e risposta.**
7. **Nomina di un responsabile della sicurezza.**

Recepimento della Direttiva NIS 2

NIS 2 - Impatto operativo – Parte 1

1. **Revisione dei processi interni.** Le PA devono aggiornare processi, piani di risposta agli incidenti e protocolli di gestione del rischio, assicurando la continuità operativa anche in caso di attacchi:
    1. **Redazione Piano Continuità Operativa;**
    2. **Redazione Business Continuity con Ruoli e Responsabilità;**
    3. **Redazione Business Impact Analysis (BIA**) (le funzioni dell'Ente che sono critiche per il normale svolgimento delle operazioni e consente di valutare l'impatto economico ed operativo in caso di interruzione – aggiornamento del Piano Continuità Operativa anche con i servizi critici in Cloud);
    4. **Redazione Piano delle Soluzioni per la Continuità Operativa;**
    5. **Redazione Piano di Disaster Recovery;**
    6. **Redazione Asset Inventory;**
    7. **Redazione Documento di Cyber security policy.** * (si veda la descrizione dettagliata nelle pagine successive)**.**

NIS 2 - Impatto operativo – Parte 2

2. **Gestione della supply chain.** Cresce l'attenzione sulla sicurezza dei fornitori e dei subappaltatori**;**

3. **Formazione e consapevolezza.** La direttiva promuove una cultura diffusa della cybersicurezza, con formazione continua e simulazioni di incidenti per tutto il personale.

4. **Aggiornamento tecnologico.** Molte PA dovranno investire nell'aggiornamento delle infrastrutture, adottando tecnologie di monitoraggio avanzate e sistemi di autenticazione forte.

5. **Sanzioni per mancato adeguamento.** Fino al 2% del fatturato per le entità essenziali, con possibilità di sospensione dei servizi e obblighi correttivi imposti dalle autorità. L'ACN effettuerà ispezioni e controlli per verificare il rispetto degli obblighi.

Recepimento della Direttiva NIS 2

UN DOCUMENTO DI POLICY DI CYBERSECURITY definisce le regole e le linee guida per proteggere le risorse digitali e le informazioni sensibili di un'organizzazione, è fondamentale per creare una cultura di sicurezza e garantire la conformità alle normative, come il GDPR e la recente Legge Italiana sulla Cybersecurity (Legge 90/2024 - NIS2).

Cosa include un documento di policy:

1. **Scopo e ambito;**
2. **Regole d'uso;**
3. **Gestione degli accessi;**
4. **Protezione dei dati;**
5. **Gestione degli incidenti;**
6. **Conformità: Assicura il rispetto di leggi e normative, come il GDPR e le direttive europee (es. NIS2).**
7. **Responsabilità.**

Recepimento della Direttiva NIS 2

Punti chiave del DOCUMENTO DI POLICY DI CYBERSECURITY:

1. **Responsabilità:** La policy stabilisce chiaramente le responsabilità di ogni persona all'interno dell'organizzazione.
2. **Cultura della sicurezza:** Promuove la consapevolezza della sicurezza e incoraggia comportamenti proattivi.
3. **Flessibilità**: Le regole devono essere adattate alla specifica realtà aziendale e ai rischi identificati attraverso un'analisi dei rischi**.**
4. **Standard di riferimento:** Spesso **si fa riferimento a standard internazionali come l'ISO 27001** che è uno standard internazionale per la certificazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Recepimento della Direttiva NIS 2

Certificazione ISO/IEC 27001:2022 in confronto alla NIS2

La certificazione ISO/IEC 27001:2022 è quindi uno standard internazionale che fornisce alle aziende un framework (struttura di base) e certifica la gestione della sicurezza delle informazioni.

Differenze chiave e integrazione tra NIS 2 e ISO/IEC 27001:2022

Nonostante molte similitudini, tra cui la gestione del rischio e la governance, **esistono differenze fondamentali:**

- **Ambito di applicazione**: la NIS 2 si concentra sui settori critici e infrastrutture essenziali, mentre la ISO/IEC 27001 è applicabile a qualsiasi azienda, indipendentemente dal settore**.**
- **Obblighi di segnalazione**: la NIS 2 impone un obbligo legale di notifica degli incidenti, mentre la ISO/IEC 27001 non lo prevede esplicitamente.
- **Resilienza operativa: la NIS 2 pone maggiore enfasi sulla capacità di recupero operativo in caso di attacco.**

Recepimento della Direttiva NIS 2

La NIS 2 e il Regolamento 2024/2690 impongono alle Pubbliche Amministrazioni un salto di qualità nella gestione della cybersicurezza, con obblighi più stringenti, responsabilità dirette per i vertici, maggiore attenzione alla gestione dei rischi e alla continuità dei servizi, e un approccio strutturato alla formazione e alla collaborazione con le autorità di settore**.**

Visto l'importanza della NIS2 ed in previsione di un ampliamento dei soggetti coinvolti con tale direttiva, a Luglio 2025 si sono affidati dei servizi di supporto specialistico al fine di aiutare l'ente a valutare in maniera esaustiva il rischio cybersecurity della Provincia in conformità con le best practices prese a modello dalla normativa NIS2 e poter così procedere alle integrazioni tecniche e strumentali per essere conformi alla normativa.

Recepimento della Direttiva NIS 2

Anche se non si è obbligati, questa operazione servirà a creare una cultura di sicurezza consolidata nell'ente e che la aiuterà nelle sfide presenti e future di Cyber sicurezza.

Tale azione sarà suddivisa in 6 Fasi così riassunte:

Fase 1 - Set-up e analisi preliminari, servirà a validare lo scopo di intervento, le tempistiche di dettaglio e i soggetti da coinvolgere

Fase 2 - Gap Analysis, servirà a Identificare i Gap (divari) di sicurezza rispetto alla NIS 2 delle infrastrutture digitali.

Fase 6 (in concomitanza con la Fase 2) Ethical Hacking, servirà a valutare lo stato di esposizione alle vulnerabilità dei sistemi e le piattaforme cloud Internet-facing (accessibili da internet) utilizzate dalla Provincia e presenti nel range di indirizzi IP condivisi dall'ente per la parte External,

Recepimento della Direttiva NIS 2

Fase 3 - Cyber Risk Assessment, servirà ad identificare e valutare le minacce e i principali scenari di rischio cyber che potrebbero impattare i sistemi e l'infrastruttura IT della Provincia di Perugia;

Fase 4 Remediation Plan & Reporting, servirà a definire il piano di intervento per implementare le azioni necessarie definendo lo sforzo lavorativo, le tempistiche ed il budget necessario,per raggiungere la conformità con le Best Practices prese a modello dalla NIS2;

Fase 5 Attività di Formazione, predisposizione della formazione personalizzata in base alle esigenze della Provincia di Perugia;

Ed Infine **Stesura del documento della Cyber Policy**, documento in cui si specificano i ruoli e le operazioni per implementare la Cyber Security ed i ruoli e le operazioni da eseguire durante un attacco informatico, esempio esfiltrazione di dati (data breach).

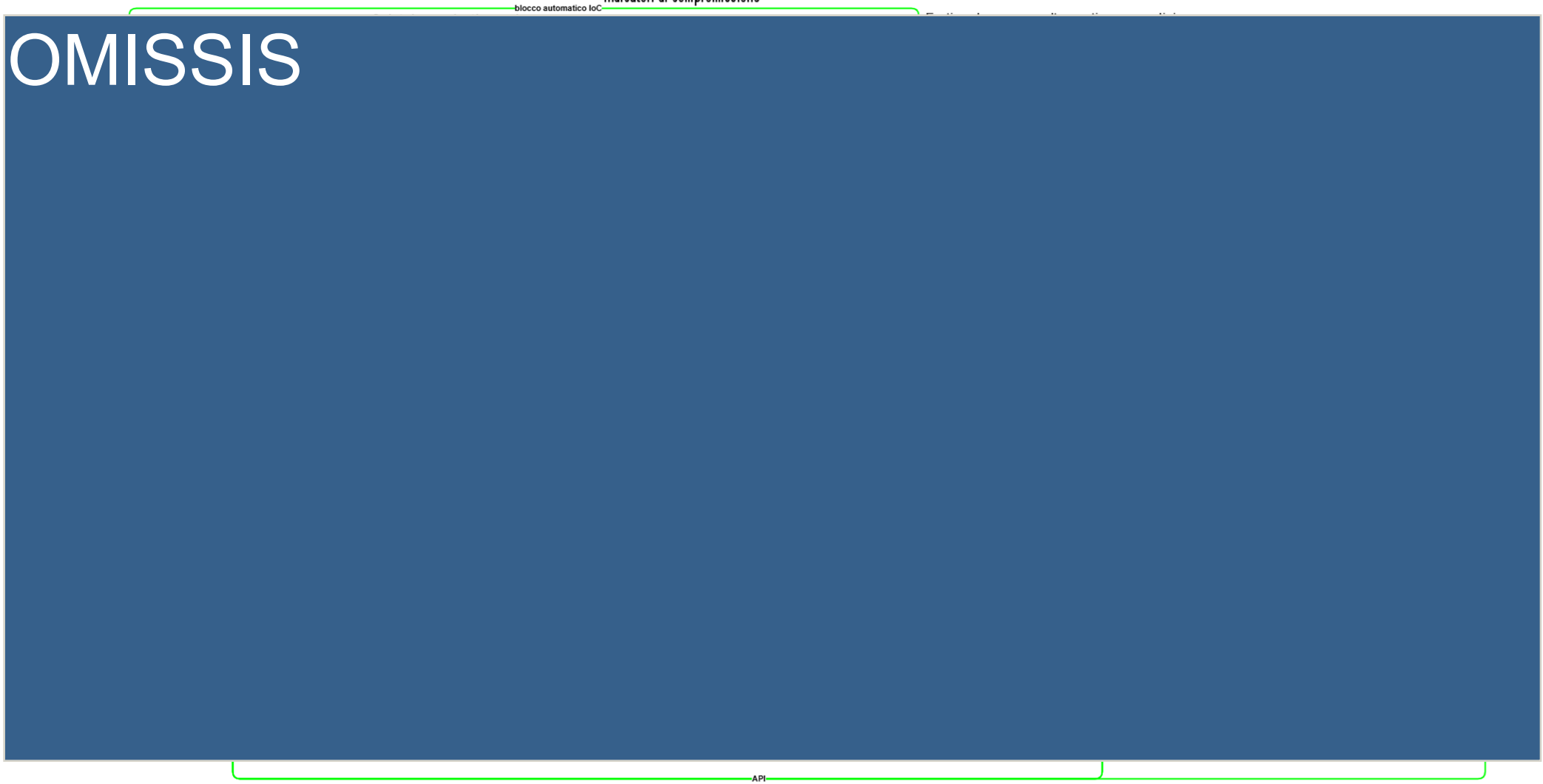
Recepimento della Direttiva NIS 2

Riflessioni sulla Direttiva NIS 2:

- **Approccio proattivo alla sicurezza informatica;**
- **Collaborazione istituzionale;**
- **Verso una cultura consolidata della cybersecurity**

Riguardando l'Impatto operativo che la NIS2 ha sull'ente, la Provincia di Perugia ha investito molto sull'aggiornamento tecnologico ed infrastrutturale, adottando tecnologie di monitoraggio avanzate e con l'attivazione di un servizio SOC - Security Operations Center – attivo 24 ore su 24 che si integra con il Servizio SIEM per la prevenzione di incidenti e per un pronto intervento (anche in maniera automatica) in caso di incidente.

Schema Infrastruttura di Monitoraggio SIEM + SOC



Concludiamo dicendo che:

- **Il PNRR 1.2 Cloud** Ha avuto una grossa spinta nel completare la migrazione dei servizi «poco sicuri» on-premise a servizi molto più sicuri in Cloud ed ha avuto un grosso impatto sulla sicurezza e sulla resilienza dei Servizi Informativi dell'ente;
- **L'ente inoltre ha stipulato un'assicurazione** per poter avere un risarcimento nella possibile eventualità di perdita di dati in caso di incidente informatico.

Grazie per l’attenzione.