GDRP Italia
Operatori e consulenti

Summer Meeting 2018

Ing. Santo Lo Piparo
Data Protection Consultant

Dott. Alessandro Feltrin
Risk manager

GDPR: SUL CONCETTO DI RISCHIO E BILANCIAMENTO DEGLI INTERESSI

Approcci aziendali sul rischio:

L'**IT** valuta il rischio qualitativamente, effettuando in primo luogo un inventario degli asset e classificando, per gli stessi, le minacce

Il **Manager** stima come l'effetto dell'incertezza impatta sugli obiettivi o la probabilità che un evento (potenzialmente dannoso) accada per il costo delle sue conseguenze

Le due visioni non tengono conto del Bilanciamento degli interessi che deve essere «misurato» nelle azioni/trattamenti dei dati rilevabili in ogni azione aziendale. Il percorso di adeguamento è caratterizzato da variabili e aspetti che talvolta non trovano nell'immediato una risposta tecnica e/o organizzativa adeguata.

GDPR ASPETTI PRELIMINARI

01 Maggiore salvaguardia e attenzione ai diritti del soggetto del trattamento, ergo maggiore protezione e sicurezza

02 Necessità di un ripensamento dell'organizzazione aziendale per interpretare il regolamento nel proprio contesto

03 Ampi margini di azione al titolare nell'attuare misure di protezione in maniera adeguata ai rischi valutati (responsabilizzazione)

04 Maggiore burocratizzazione: testimoniare esternamente l'implementazione di controlli e stimolare internamente un atteggiamento proattivo o risk-based

Santo Lo Piparo – Alessandro Feltrin

COS'E' IL RISCHIO INFORMATICO

Per "rischio informatico" si intende qualsiasi rischio di perdita finanziaria, interruzione o danno alla reputazione di un' organizzazione a causa di un qualsiasi tipo di guasto dei suoi sistemi informatici.

La percezione del rischio informatico è una degli aspetti aziendali più difficili da far accettare in un ambiente organizzativo.

L'idea che «se le operazioni correnti sono sicure per me, allora è sicuro per tutti» non è più vera in epoca di GDPR.

La percezione del rischio informatico, troppo spesso è maturato solo dopo il determinarsi di una DANNO per l'organizzazione.

GDPR: ARTICOLO 32.1 SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

A. la pseudonimizzazione e la cifratura dei dati personali;

B. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

C. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

D. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

GDPR: ARTICOLO 32.1 SICUREZZA DEL TRATTAMENTO

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Obbligo di attuare misure di sicurezza adeguate in considerazione dei seguenti elementi:

- Lo stato dell’arte e i costi di attuazione
- La natura e il campo di applicazione del trattamento
- Il contesto e le finalità del trattamento
- Il rischio, la probabilità e la gravità delle conseguenze per i diritti e le libertà delle persone

GDPR SICUREZZA DEI DATI

Art. 5 (1)(b)

Lo scopo per il quale si stanno raccogliendo i dati personali

Art. 5 (1)(d)

Mantenere i dati sempre aggiornati e corretti

Art. 5 (1)(f)

Evitare qualsiasi operazione non autorizzata o contraria alla legge

Art. 5 (2)

Essere in grado di dimostrare ottemperanza delle norme del GDPR quando richiesto

Arti. 4 (1)

Implementare le adeguate misure tecnico-organizzative

Art. 25 (2)

I dati personali dovrebbero essere processati solo per lo scopo per il quale sono stati raccolti

GDPR SICUREZZA DEI DATI

Art. 30

Mantenere uno storico di tutte le operazioni avvenute sui dati

Art. 32(1)(a)

Assicurare sempre confidenzialità e criptare i dati quando necessario

Art. 32(1)(b)

Assicurare la disponibilità, confidenzialità e integrità dei dati in ogni fase

Art. 32(1)(d)

Testare ciclicamente l'efficacia delle misure di sicurezza adottate

Art. 32(2)

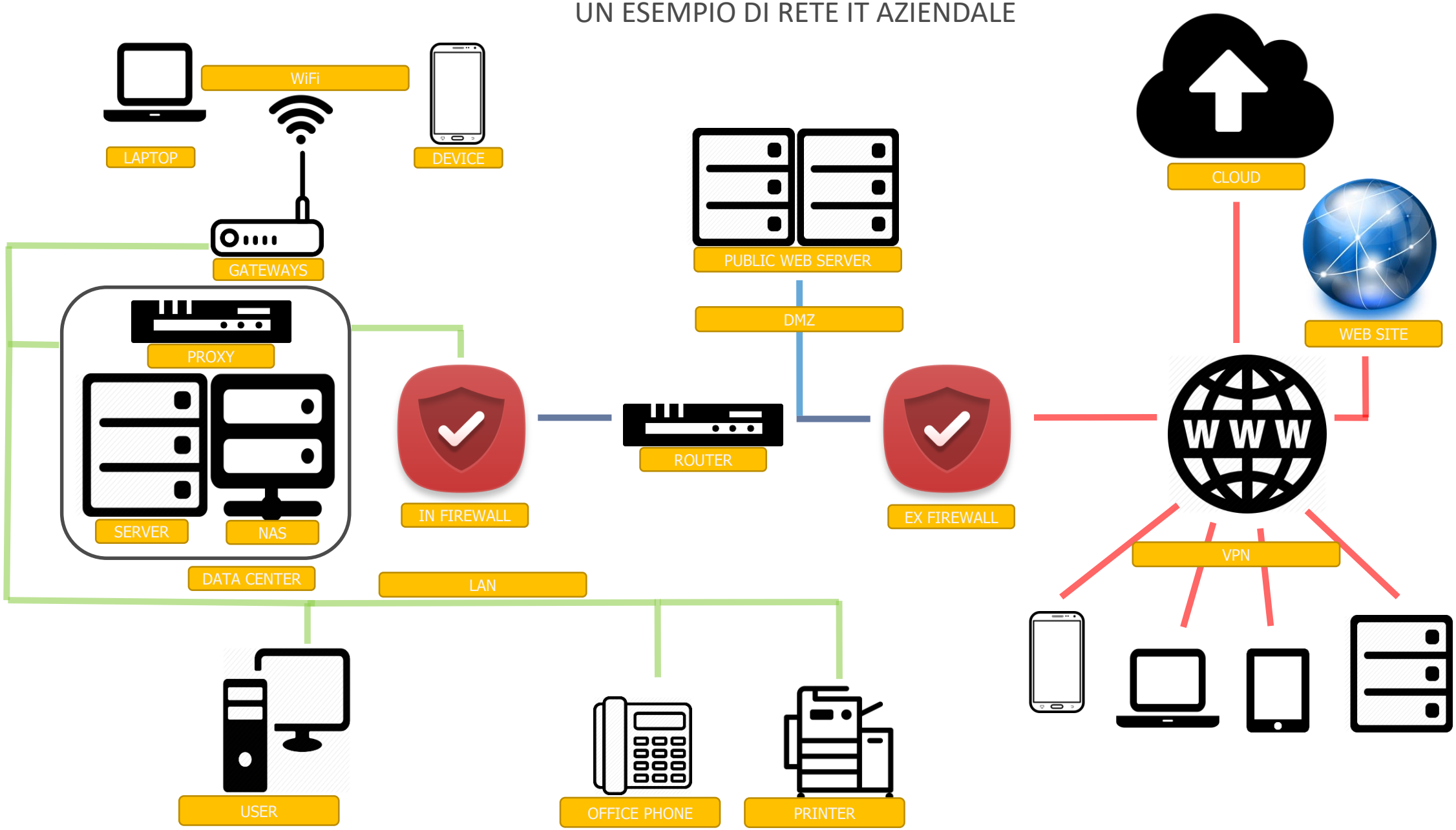
Implementare un piano di gestione dei rischi, che ponga in essere meccanismi di controllo

Art. 33

In caso di violazione, informare tempestivamente le autorità competenti entro 72 ore

Santo Lo Piparo – Alessandro Feltrin

UN ESEMPIO DI RETE IT AZIENDALE



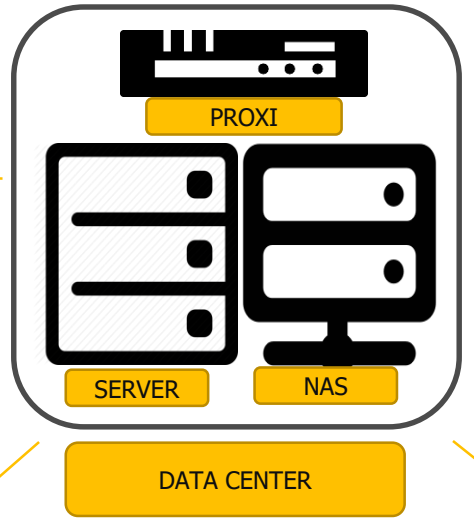
UNA RETE IT AZIENDALE – LA SICUREZZA

DIFESE FISICHE

Rilevatori di fumo ed incendio e umidità

Separazione delle aree – Accessi controllati

Certificazioni degli impianti e delle reti



Sistemi anti-intrusione

Protezione fisiche

Sistemi di raffreddamento e climatizzazione

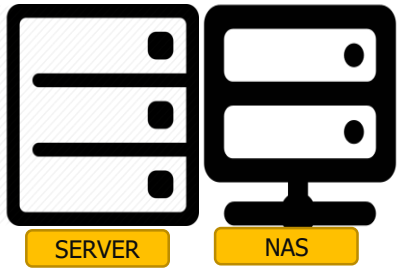
UNA RETE IT AZIENDALE – LA SICUREZZA

CONTINUITA' OPERATIVA

Alimentazione e continuità di energia

Mirroring

Testing - Restore



Backup e loro storaggio

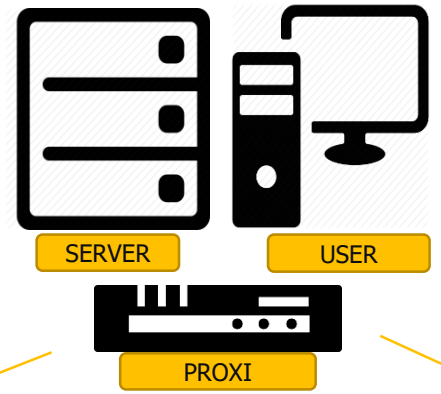
Ridondanza dei dati

Management plan

Santo Lo Piparo – Alessandro Feltrin

UNA RETE IT AZIENDALE – LA SICUREZZA

SICUREZZA LOGICA



- Monitoring degli accessi – data log
- Management degli incidenti: Log Files -
- Gestione degli accessi
- Antivirus –Antimalware
- Identificazione ed autenticazione degli utenti
- IDS: Intrusion Detection System
- Limitazione di traffico
- Cifratura o criptografia dei dati
- Gestione degli archivi, manutenzione e distruzione dei dati
- Penetration test

UNA RETE IT AZIENDALE – LA SICUREZZA

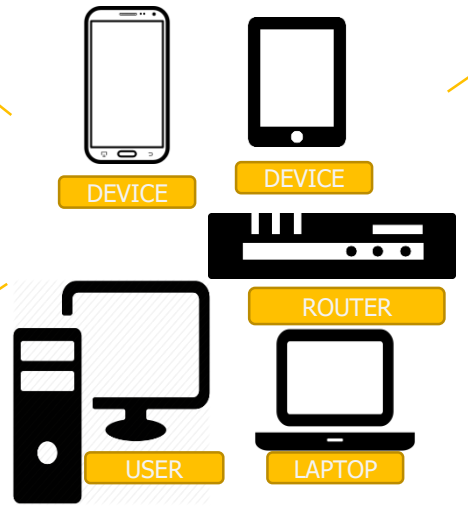
SICUREZZA LOGICA

Strumenti tecnologici per mettere in sicurezza tutti gli asset che gestiscono dati personali.

Una soluzione specifica per identificare e gestire le vulnerabilità che possono sorgere nel tuo ambiente

Un sistema di monitoraggio degli asset e dei sistemi che gestiscono dati personali

Dotarsi di una procedura standard per identificare, rispondere prontamente e creare un report nel caso in cui si verifichino infrazioni.



Sistemi in grado di gestione di un registro di tutte le attività che interessano la data protection

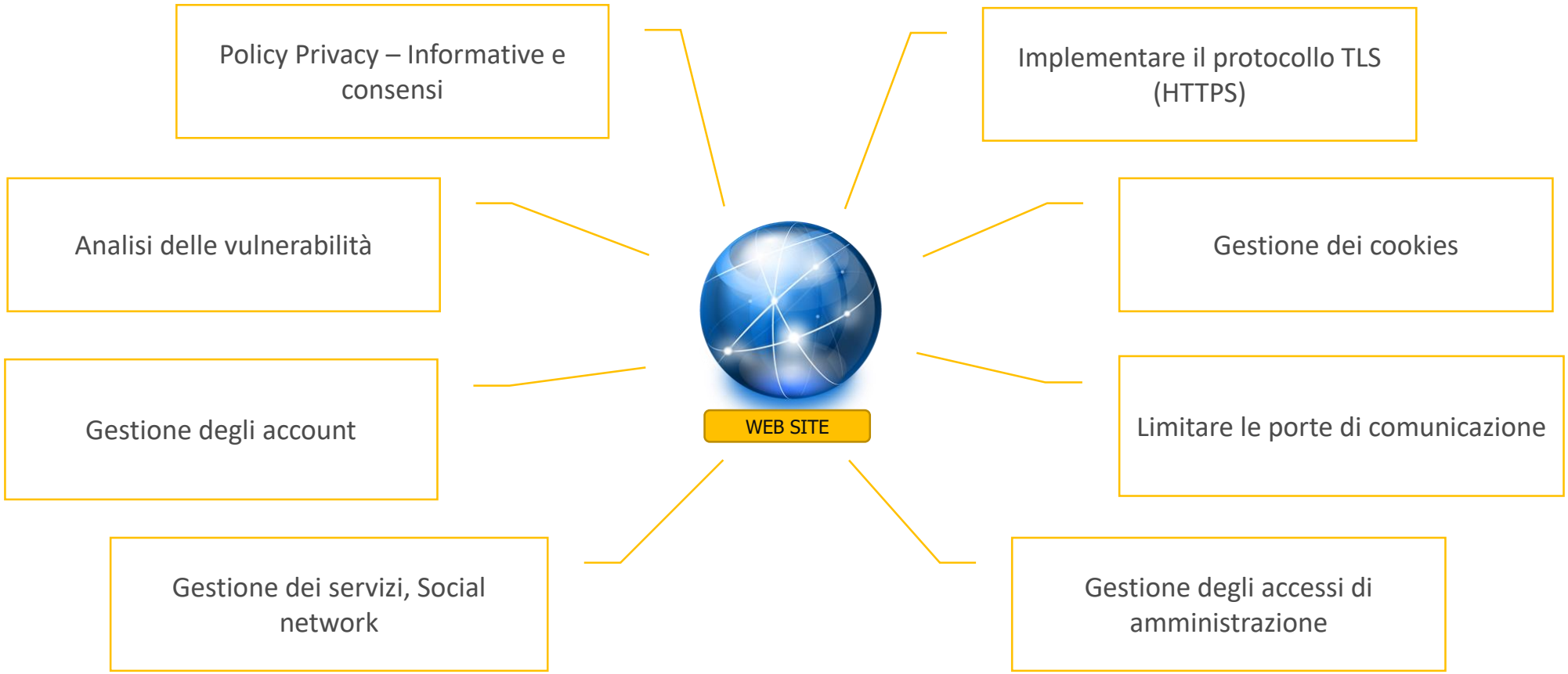
Rendere sempre identificabile l'utente che attraverso account privilegiati ha accesso a dati sensibili

IDS: Intrusion Detection System

Adottare adeguate misure di sicurezza e criptografia per i dati personali in transito nel tuo ambiente.

UNA RETE IT AZIENDALE – LA SICUREZZA

WEBSITE



UNA RETE IT AZIENDALE – LA SICUREZZA

GESTIONE DELLA SICUREZZA E DELLA CONSAPEVOLEZZA

- Organigrammi, Incarichi
- Informazione e formazione
- Adeguamento alla tecnologia esistente
- Documentazione, evidenze, procedure istruzioni
- Procedure per il controllo e il monitoraggio
- Policy, Regolamenti interni
- Manutenzione preventiva
- Informative e consensi in relazione al trattamento

Grazie