LAN SERVICE group

Clusit
Associazione Italiana per la Sicurezza Informatica

Gestione del rischio e nuovi scenari di attacco: evitare il Data Breach ed essere conformi alla GDPR

Francesco Speciale

Evento Clusit Verona
4 ottobre 2017

LAN SERVICE group

Trasformiamo esigenze in soluzioni

In integrazione. In consulenza

In funzionalità. In interazione

In connettività. In cloud

Il gruppo

LAN SERVICE CLOUD SOLUTIONS

ACKTEL CREATIVE WEB SOLUTIONS

evolution Lightspeed Internet Solutions

50	persone
3	brand
6 mil/€	fatturato consolidato
Casale M.to	sede principale
Milano	sede operativa
Lugano	sede operativa

Certificazione ISO 9001:2008
"Progettazione, realizzazione di infrastrutture di rete e servizi di gestione"

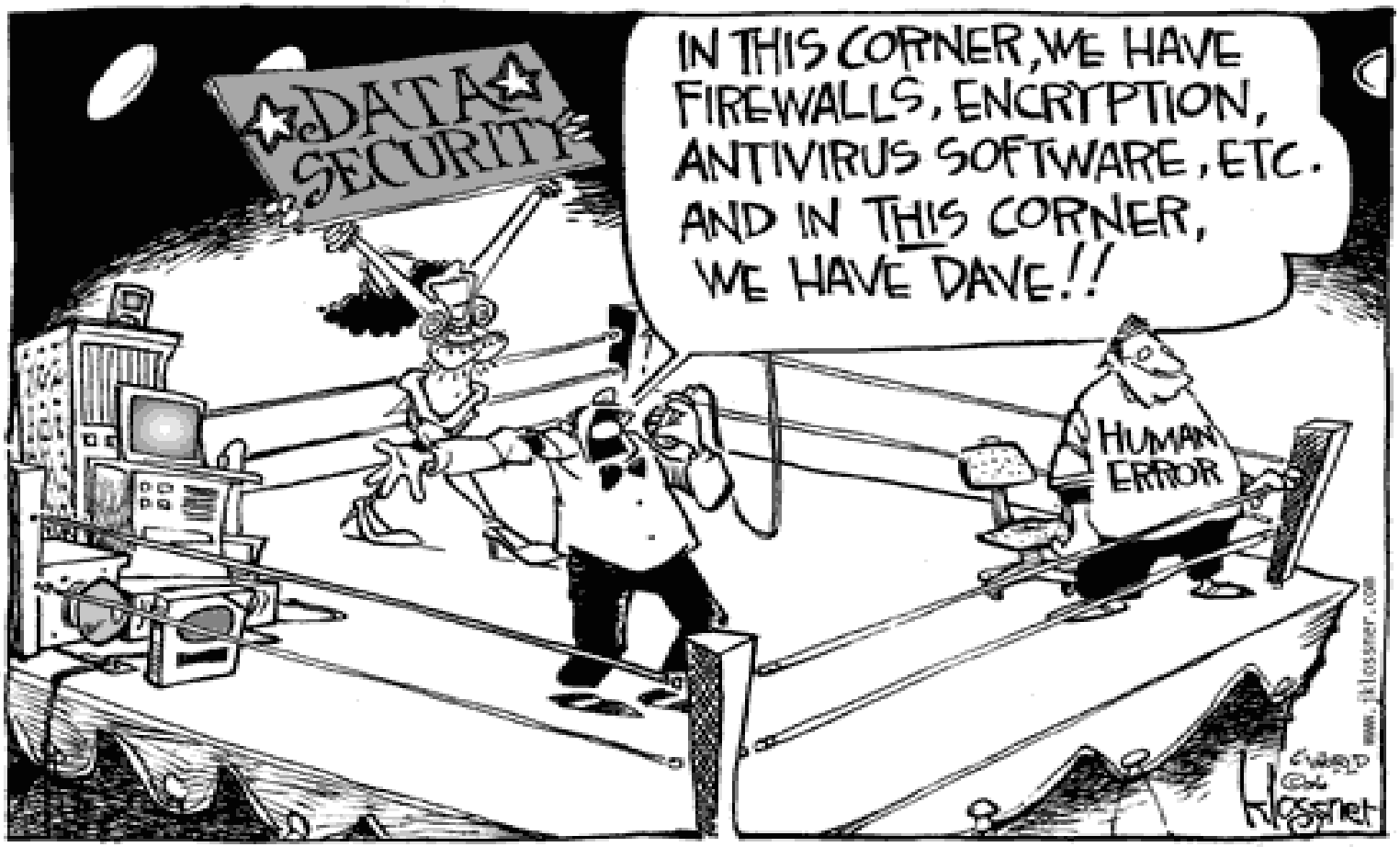
Certificazione ISO 27001
"Sicurezza delle informazioni"

www.lanservicegroup.it

Clusit Associazione Italiana per la Sicurezza Informatica

LAN SERVICE group

La Sicurezza è un concetto sempre più relativo ...



Metodologia LAN Service: c'è un filo rosso ...

Aspetto Tecnologico	Aspetto Normativo	Aspetto Organizzativo
Azioni preventive (Risk Assessm., Vulnerability M.)	Compatibilità Azienda con GDPR ad oggi	Nuovi ruoli in azienda (DPO) e nuovi tipi docum.
Implementare l'Ecosistema della sicurezza	Nuovi Team multidisciplinari in Azienda	Azione di dialogo con interessati e Autorità Garante
Eseguire il Backup e Recovery dei dati periodicam.	Sfruttare il GDPR ed Industria 4.0 come opportunità	Pianificare corsi di formazione permanenti

Comparazione Codice Privacy vs. GDPR

Codice della Privacy ITA D.Lgs. 196/2003	GDPR EUR 679/2016
Adottare misure minime sicurezza	Accountability: misure adeguate
Prima defin. di Tratt. Dato Personale	Privacy by Design / by Default
Nuovi criteri Informativa e Consenso	Analisi Rischio Digitale (DPIA)
Nessuna figura di Riferimento	Nuova Figura DPO (D.P. Officer)
Si confronta con normative Privacy	Obbligo comunicaz. Data Breach 72h
Maggiore tutela per dati Sensibili	Trasferimenti dati in paesi Extra EU
Appena nato il Mercato Digitale	Sanzioni da medio-grande Azienda

La Nuova figura del DPO (Data Protection Officer)

Il DPO deve essere designato nei seguenti casi:

- in tutte le autorità pubbliche
- nelle organizzazioni che effettuano un monitoraggio sistematico su larga scala
- nelle organizzazioni che coinvolgono l'elaborazione su larga scala di dati particolari

Possono essere interni o esterni.
Dovranno avere **qualità professionali**, un'approfondita **conoscenza della normativa e delle prassi in materia di privacy** ed operare **in autonomia ed indipendenza**.

Minimizzare i Rischi dell'Organizzazione

Come fare a minimizzare i rischi? Alcuni esempi concreti:

- Incontrare le aree MKTG e Sales regolarmente e sempre prima che vengano avviate le loro iniziative
- Tenere aggiornato e completo il **Registro dei trattamenti**, il nuovo registro che serve innanzi tutto a documentare dinanzi all'Autorità di Controllo (Garante della Privacy) la conformità dell'organizzazione alle norme del Regolamento GDPR
- Formare il personale con dei corsi sulla sicurezza ricorrenti (es. CBT) che espongano tutti i vari rischi
- Controllare con regolarità se i dati personali debbano essere cancellati (es. non più necessari alla finalità, oppure per decesso dell'interessato o su sua richiesta)

Caso Equifax

Equifax è un'agenzia USA quotata in Borsa attiva nel controllo dei crediti. A fine luglio 2017 quasi la metà dei cittadini americani (143 milioni di cittadini), sono stati informati che il loro **Social Security Number ed i loro dati personali** erano stati violati e potenzialmente utilizzati a loro danno da chiunque volesse truffarli. Un Data Breach colossale.

Sottovalutati molti rischi e cattiva gestione della comunicazione verso l'esterno:

- Password deboli e facilmente violabili
- Dati non cifrati o comunque mascherati
- Gravi vulnerabilità in una o più applicazioni Web, alcune già note da mesi
- Comunicazione alle Autorità del Data Breach dopo 6 settimane
- Comunicazione su Twitter non aggiornata alla luce del Data Breach

Risultati:

- Immediato crollo del 30% in Borsa del valore del titolo Equifax
- avviata una class action con la richiesta di un risarcimento di $70 miliardi basata sull'accusa di negligenza in tema di investimenti in Cybersecurity
- Dimissioni in massa di CEO, CIO, CISO ed altri Top Manager

Normative simili al GDPR sono entrate in vigore in altre aree del mondo come in Russia ed altri stati extra-Europa. Ma allora **vale la pena risparmiare le risorse sulla sicurezza anno su anno e poi dover affrontare comunque miliardi di danni da risarcire e la propria immagine compromessa**?

Ormai la protezione dei dati e le strategie di sicurezza devono essere **affrontate in modo sistemico e permanente**, coinvolgendo diversi ruoli aziendali e promuovendo una **cultura della sicurezza** che possa permeare le diverse aree delle organizzazioni. Altrimenti le sanzioni (fino al 4% del fatturato mondiale) ed i danni d'immagine che bisogna affrontare sono proibitivi.

LAN SERVICE group

Clusit
Associazione Italiana per la Sicurezza Informatica

Francesco Speciale
francesco.speciale@lanservice.it

GRAZIE.

Bitdefender®

Soluzione Bitdefender Gravity Zone Enterprise

Un primario gruppo italiano leader mondiale nei sistemi di confezionamento aveva l'esigenza di rafforzare le proprie soluzioni di sicurezza alla luce di una costante espansione internazionale che ha già raggiunto oltre 60 mercati mondiali e 900 clienti nel mondo serviti attraverso 4 impianti produttivi.

Esigenze del cliente

- **Proteggersi dagli attacchi di nuova generazione**
- **Implementare un sistema di DOPPIA PROTEZIONE a livello dei client, dei server fisici e degli Hypervisor**
- **Proteggere le stazioni VDI 3D fondamentali per le esigenze di progettazione e prototipazione del cliente**
- **Gestire tutto il ciclo della sicurezza includendo i momenti di:**
  - **Identificazione**
  - **Protezione**
  - **Rilevamento**
  - **Risposta**
  - **Recupero**

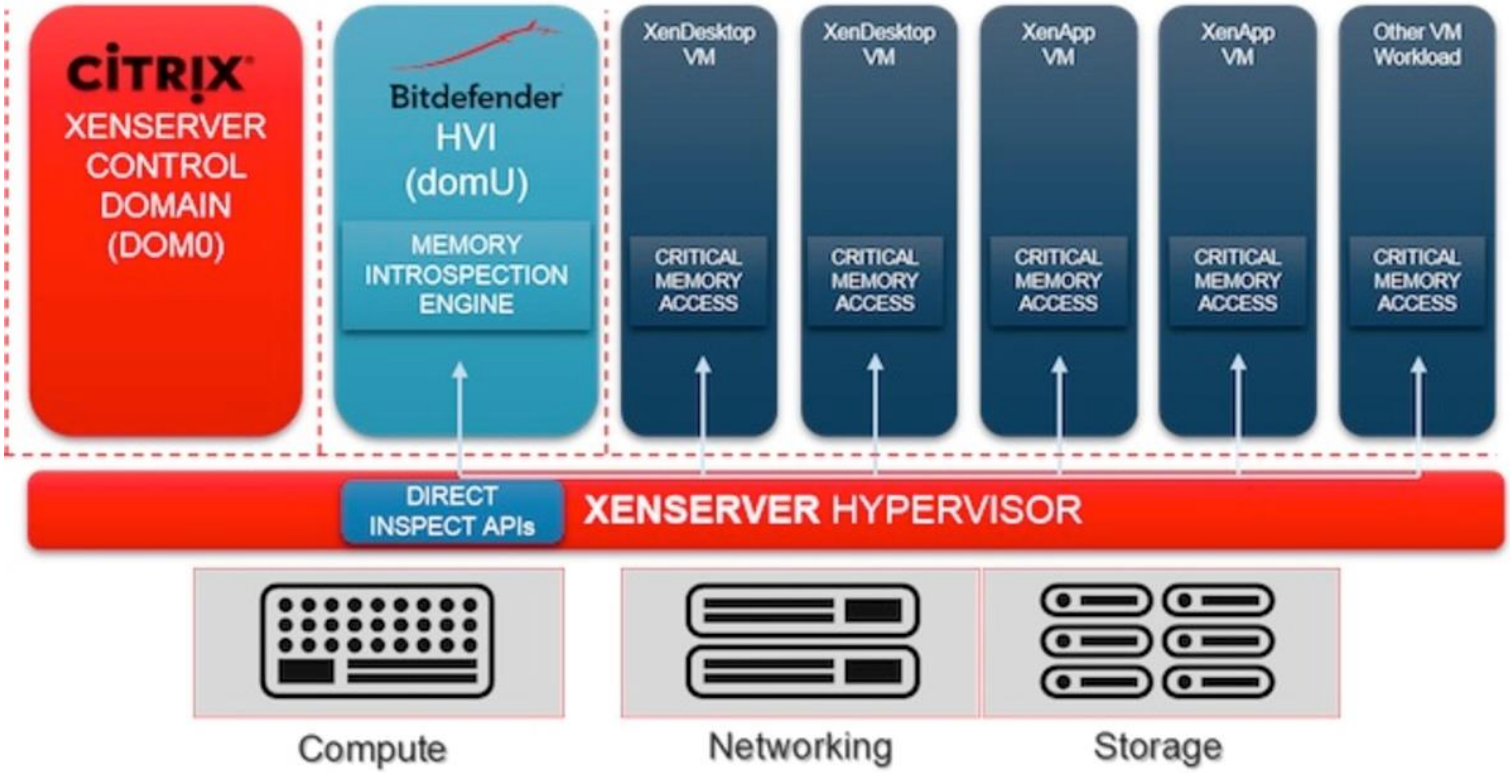
Soluzione Bitdefender GravityZone Enterprise

Nuovo livello di riferimento per la sicurezza

Cosa abbiamo realizzato?

- Abbiamo implementato **GravityZone Enterprise** rispondendo alle esigenze del cliente in termini di risposta agli **attacchi di nuova generazione**, grazie alle tecnologie di Machine Learning (ML) ed alle analisi comportamentali della Suite Bitdefender GravityZone, e potendo gestire l'intero ambiente in modo semplice da un'unica console centrale.

Bitdefender Hypervisor Introspection (HVI)



Tecnologia esclusiva

- **Bitdefender Hypervisor Introspection**, prima ed esclusiva soluzione di sicurezza, agentless, in grado di funzionare **interamente dall'esterno del sistema operativo**, sfruttando le API di Citrix XenServer Direct Inspect.

Bitdefender GravityZone Endpoint Security HD

- GravityZone Endpoint Security HD è stato adottato **perché blocca le minacce sconosciute e rileva gli attacchi mirati** in grado di eludere le altre soluzioni di sicurezza per endpoint, utilizzando un avanzato apprendimento automatico,un'analisi comportamentale ed un'ampia gamma di tecnologie non basate sulle firme.

- Nel momento in cui ha rilevato la minaccia, **Endpoint Security HD effettua un'azione immediata**, come per esempio il ripristino di modifiche eventuali risultate dannose per il ritorno alla normale operatività.

- Sfrutta la tecnologia esclusiva **HyperDetect™** contro Ransomware, Phishing, attacchi basati su script, Exploit, Malware

Vantaggi di Bitdefender GravityZone Enterprise

Vantaggi ottenuti

- Raggiungimento dei più elevati standard di sicurezza (es. NIST) e protezione dagli attacchi di NUOVA GENERAZIONE
- Doppia protezione dei client e dei server fisici e virtuali
- Nessun impatto sulle performance dei sistemi VDI 3D (grazie ad HVI)
- Protezione del network delle varie sedi locali e remote mediante la console di gestione centralizzata
- Unificazione della soluzione di sicurezza in un unico prodotto
- Forte riduzione del TCO
- Miglior rapporto costo/prestazioni sul mercato

LAN SERVICE group

Clusit
Associazione Italiana per la Sicurezza Informatica

Stefano Maranzana
stefano.maranzana@lanservice.it

GRAZIE.

Bitdefender®