Regolamento UE 2016/679 Sicurezza Informatica

28 Marzo 2018

Cronaca 1/4

TGCOM24 MEDIASET Martedì 20 Marzo

Tgcom24 | Mondo

19 MARZO 2018 06:30

Dati Facebook usati per manipolazioni elettorali, Wall Street punisce il titolo

Lo scandalo Cambridge Analytica affonda in Borsa la società di Zuckerberg. Un ex dipendente dell'azienda di consulenza britannica svela alchimie e algoritmi per creare fake news "ad alto livello"

(297) LEGGI DOPO COMMENTA

Facebook crolla a Wall Street per lo scandalo Cambridge Analytica: il titolo del gigante dei social media è arrivato a perdere oltre il 7% sulla scia delle rivelazioni su Cambridge Analytica, una società che avrebbe aiutato, sfruttando i dati di oltre 50 milioni di utenti Fb, Donald Trump durante le elezioni del 2016 e favorito, in Gran Bretagna, la campagna pro Brexit. Alex Stamos, a capo della sicurezza delle informazioni di Fb, si è dimesso.

R.it | Esteri

Home | Politica | Economia | Sport | Spettacoli | Tecnologia | Motori | Tutte le sezioni | D | Rep tv

Brexit »


Facebook, crollo a Wall Street dopo lo scandalo Cambridge Analytica. Verso


Brexit, Barnier: "Abbiamo un accordo per transizione fino al 2020"


Unilever non avrà più una sede legale a Londra, ultimo effetto della


Il paradosso della Mini: la dura legge de dazi si abbatt sulla Gran

187

Facebook, crollo a Wall Street dopo lo scandalo Cambridge Analytica. Verso l'addio il capo della sicurezza Stamos

(afp)

Titolo in calo del 6,8% dopo l'inchiesta giornalistica che ha rivelato che sarebbero stati acquisiti illegalmente dati di 50 milioni di utenti del social network. Stamos dovrebbe lasciare ad agosto: "Ho già cambiato ruolo". Il Garante britannico per l'informazione vuole perquisire gli uffici della società

Cronaca 2/4

Cambridge Analytica e Facebook. I dati personali valgono oro ma le persone li regalano

di Roberto Pezzali - 19/03/2018 12:07 6

I dati di 50 milioni di utenti Facebook sarebbero stati rivenduti illegamente e usati per pilotare le elezioni presidenziali. Dietro tutto questo una società inglese, la Cambridge Analytica, che per farlo ha sfruttato lo scarso controllo della piattaforma sui dati in suo possesso.

Facebook, crollo a Wall Street dopo lo scandalo su Cambridge Analytica. NYT: si dimette il capo della sicurezza Stamos

(ansa)

Titolo in calo del 6,8% dopo l'inchiesta giornalistica che ha rivelato che sarebbero stati acquisiti illegalmente dati di 50 milioni di utenti del social network. La Borsa Usa in forte calo. Parla Kogan: "Non sono una spia"

Cronaca 3/4


WIRED .IT
Sezioni
Wired Next Fest
Gallery
Video
HOT TOPIC
WIRED HEALTH
STEPHEN HAWKING
FACEBOOK
DIZIONARIO DIGITALE
SPORT
ELEZIONI 2018
GOOGLE
SERIE TV
AMAZON...
VEDI TUTTI
HOME
ATTUALITÀ
POLITICA
Perché il caso Cambridge Analytica dovrebbe preoccupare anche te
Un quiz su Facebook fatto da 270mila persone ha portato alla profilazione di 50 milioni di utenti. Ecco perché il caso Cambridge Analytica riguarda anche te
di Philip Di Salvo
Ricercatore e giornalista
19 MAR, 2018

Cronaca 4/4

Falla? Quale falla?

I giornalisti del *Guardian* dicono di avere ricevuto forti pressioni da Facebook nei giorni prima della pubblicazione degli articoli, soprattutto per non definire "falla" il meccanismo che consentì a Kogan e poi a Cambridge Analytica di ottenere quell'enorme quantità di dati. Una singola parola può sembrare poca cosa, ma in realtà è centrale in questa vicenda. Da un punto di vista prettamente informatico e di codice non c'è stata nessuna falla: Kogan non ottenne i dati sfruttando qualche errore o buco nel codice che fa funzionare Facebook, semplicemente sfruttò un sistema che all'epoca era lecito e contemplato nelle condizioni d'uso. L'integrità informatica di Facebook non è stata quindi violata in nessun modo, e su questo punto i suoi responsabili puntano comprensibilmente molto per tranquillizzare gli utenti e ridimensionare l'accaduto. D'altra parte, non si può negare che le condizioni d'uso di Facebook fossero "fallate", visto che permettevano una raccolta di informazioni sproporzionata e senza che se ne potessero rendere facilmente conto le persone comprese nelle reti di amici. Il fatto che la pratica fosse lecita non riduce la sua portata o gli effetti che poi nei fatti ha avuto.

Caso isolato?


The New York Times

Russian Hacking in the U.S. Election

Complete coverage of Russia's campaign to disrupt the 2016 presidential election.


The Telegraph

Business

Half a billion Yahoo users' data stolen in 'state-sponsored' hack


theguardian

UK hit by 188 high-level cyber-attacks in three months

Sunday 12 February 2017 15.06 GMT


THE WASHINGTON FREE BEACON

China Continuing Cyber Attacks on U.S. Networks


CANADA

Federal government facing 'serious' cyber attacks from state-sponsored hackers and terrorist groups: CSIS


Forbes / #CyberSecurity

SEP 25, 2017

Are The Equifax, SEC And Deloitte Cybersecurity Breaches Desensitizing Society To This Threat?


Seeking Alpha α

Microsoft's secret database hack in 2013

Oct. 17, 2017 4:55 AM ET | About: Microsoft Corporation (MSFT) | By: Yoel Minkoff, SA News Editor

- Microsoft's (NASDAQ:MSFT) secret internal database for tracking bugs in its own software was broken into by a highly sophisticated hacking group in 2013, according to five former employees, in only the second known breach of such a corporate database.
- Spies for governments around the globe and other hackers are said to covet such information because it shows them how to create tools for electronic break-ins.


THE WALL STREET JOURNAL.

POLITICS | NATIONAL SECURITY

Russian Hackers Stole NSA Data on U.S. Cyber Defense

Agenda

- Sicurezza Informatica: la teoria
  - Concetti base: disponibilità, integrità e riservatezza
- Le minacce
  - I malware e gli attacchi informatici
- Le difese
  - Regole pratiche e software
- Conformità al nuovo regolamento
  - Cosa devo fare?
- Conclusioni
  - Caso di studio

Concetti base

Concetti base

Qualunque programma che si occupi di preservare la sicurezza delle informazioni, persegue, in qualche misura, tre obiettivi fondamentali:

- la **disponibilità**
- l'**integrità**
- la **riservatezza**

delle informazioni.

Concetti base: disponibilità

La disponibilità è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono.

Questo significa che sistemi, reti e applicazioni hanno le capacità necessarie a fornire il livello di servizio e le prestazioni richieste e che, in caso di guasto o di eventi distruttivi, sono pronti gli strumenti e le procedure per ripristinare l'attività in tempi accettabili.

Concetti base: integrità

L'integrità è il grado di correttezza, coerenza e affidabilità delle informazioni e anche il grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche.

Per le informazioni, l'integrità viene meno quando i dati sono alterati, cancellati o anche inventati, per errore o per dolo, e quando si perde, per esempio in un database, la coerenza tra dati in relazione tra loro (per esempio i record coinvolti in una transazione).

Concetti base: riservatezza

La riservatezza consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate, e si applica sia all'archiviazione sia alla comunicazione delle informazioni.

Un'informazione è composta generalmente di più dati in relazione tra di loro, ciascuno dei quali non necessariamente costituisce un'informazione.

La riservatezza dell'informazione può essere quindi garantita sia nascondendo l'intera informazione (per esempio con tecniche di crittografia) sia nascondendo la relazione tra i dati che la compongono.

LE MINACCE

Le minacce: malware

Malware (abbreviazione di malicious software) significa letteralmente software malintenzionato: indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata.

Il termine malware è stato coniato nel 1990 da Yisrael Radai.

Precedentemente veniva chiamato genericamente virus per computer

Le minacce: tipi di malware

Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Sono in grado di replicarsi autonomamente.

Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di **ingegneria sociale**, oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

Le minacce: tipi di malware

Trojan horse: deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto. I trojan non si diffondono autonomamente.

Spesso i Trojan(come pure virus e worm) hanno lo scopo di installare dei Keylogger, ossia degli strumenti di sniffing, hardware o software, in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio o di un altro computer.

Altre volte i Trojan (come pure virus e worm) installano delle Backdoor, ossia delle porte che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico.

Le minacce: tipi di malware

Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono essere di vario tipo: dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.

Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.

Dialer (nota storica): questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

Le minacce: gli attacchi informatici

Semplificando il discorso ai minimi termini:

1. Scoprire quali macchine/servizi ci sono “in giro” con la scansione attiva (usando ad esempio un software come NMAP)
2. Intercettazione del traffico (usando ad esempio un software come Wireshark)
3. Ingegneria sociale: ottenere informazioni sfruttando meccanismi sociali (meriterebbe un approfondimento)
4. Trovare le vulnerabilità dei sistemi già note (esistono database a libero accesso e con la spiegazione della procedura di attacco)
5. Sferrare l’attacco (esistono distribuzioni di Linux con tutti gli strumenti a portata di mano)

LE DIFESE

Le difese: aggiornamento dei sistemi

Da un punto di vista prettamente operativo prima di tutto bisogna accertarsi che i prodotti installati, sistemi operativi e software applicativi (ad esempio il pacchetto Office) siano coperti dal supporto del produttore.

I sistemi devono essere sempre aggiornati, altrimenti il rischio di esposizione di dati e informazioni è elevato.

Si può partire semplicemente dalla verifica dei sistemi operativi in azienda

- Utilizzate ancora Windows Xp?
- E Windows Vista?
- E Windows 7?

Le difese: aggiornamento dei sistemi

Sapete che per alcuni di questi è concluso già anche il periodo di supporto esteso?

E che per Windows 7 stesso si concluderà il supporto esteso a inizio 2020?

Sistemi operativi client	Service Pack o aggiornamento più recente	Fine del supporto Mainstream	Fine del supporto Extended
Windows XP	Service Pack 3	14 aprile 2009	8 aprile 2014
Windows Vista	Service Pack 2	10 aprile 2012	11 aprile 2017
Windows 7*	Service Pack 1	13 gennaio 2015	14 gennaio 2020
Windows 8	Windows 8.1	9 gennaio 2018	10 gennaio 2023
Windows 10, rilasciato a luglio 2015**	N/D	13 ottobre 2020	14 ottobre 2025

Ogni applicazione ha il suo ciclo di vita, perderne il controllo vi espone a rischi inutili!

Le difese: aggiornamento dei sistemi

E per Windows 10?

Cronologia delle versioni di Windows 10	Data di disponibilità	Data di fine supporto Mainstream	Data di fine supporto Extended
Windows 10 Enterprise 2016 LTSB Windows 10 IoT Enterprise 2016 LTSB	2 agosto 2016	12 ottobre 2021	13 ottobre 2026
Windows 10 Enterprise 2015 LTSB Windows 10 IoT Enterprise 2015 LTSB	29 luglio 2015	13 ottobre 2020	14 ottobre 2025

Nota: non tutte le funzionalità in un aggiornamento funzioneranno in tutti i dispositivi. Un dispositivo potrebbe non essere in grado di ricevere aggiornamenti se l'hardware del dispositivo non è compatibile, se mancano driver aggiornati o se non rientra più nel periodo di supporto dell'OEM (Original Equipment Manufacturer) per altri motivi.

Le difese: software su PDL

ANTIVIRUS

I classici Anti-virus sono normalmente composti da più parti:

1.Un **file di firme** è un archivio che contiene tutte le firme dei virus conosciuti.

2.Un **programma antivirus** -permette di eseguire su richiesta una serie di operazioni, come l'aggiornamento del database delle firme, la scansione completa del sistema o di singoli files, l'eliminazione dei file sospetti etc..

3.Un **programma di ascolto** caricato in memoria all'avvio richiama l'antivirus ogni volta che viene creato o modificato un nuovo file o una zona di memoria.

Le difese: software su PDL

ANTI-SPYWARE

Gli anti-spyware sono programmi utilizzati per eliminare dal sistema diverse tipologie di malware e in particolare spyware, adware. Le funzioni di questi programmi sono simili a quelle degli antivirus, ma non sono la stessa cosa poiché gli anti-virus propriamente detti proteggono il computer solamente da una tipologia di malware: i virus appunto.

Le difese: software su PDL

ANTISPAM

Lo spamming è l'invio di messaggi indesiderati (generalmente di tipo commerciale e pubblicitario) ed è noto anche col nome di «posta spazzatura».

Poiché lo spam viene inviato senza il permesso del destinatario ed è considerato altamente dannoso anche dagli Internet Service Provider, che vi si oppongono sia per i costi generati dal traffico indesiderato sia perché può costituire una violazione contrattuale della «Acceptable Use Policy» ed essere causa di interruzione dell'abbonamento da parte dell'utilizzatore.

Gli antispam che analizzano la provenienza e/o il contenuto dei messaggi effettuando una azione di filtraggio.

Le difese: software su PDL

2018 GARTNER MAGIC QUADRANT FOR ENDPOINT PROTECTION PLATFORMS

Gartner Inc. è una società per azioni multinazionale leader mondiale nella consulenza strategica, ricerca e analisi nel campo dell'Information Technology con oltre 60.000 clienti nel mondo. L'attività principale consiste nel supportare le decisioni di investimento dei suoi clienti attraverso ricerca, consulenza, benchmarking, eventi e notizie

Le difese: le password

I pirati informatici usano strumenti sofisticati che consentono di determinare rapidamente migliaia di probabili password con l'uso di semplici indizi ricavabili dalle caratteristiche dell'account e del suo titolare.

Generalmente è solo una questione di tempo…

BUONA REGOLA

- Lunga: almeno 8 caratteri e/o simboli.
- Includere maiuscole, minuscole, numeri e simboli.
- Non ripetere gli stessi caratteri
- Numeri e lettere scelti casualmente.
- Password diverse per contesti diversi
- Cambio frequente (max 6 mesi)

DA EVITARE

- Utilizzare in tutto in parte l'account
- Parole reali in qualsiasi lingua
- Nomi e date di nascita
- Numeri e lettere in sequenza… alfabeto
- Lettere o simboli con sequenza ricavata dalla tastiera
- Annotare la password sullo schermo
- Utilizzare la funzionalità *memorizza la password*
- Annotare la password sulla rubrica

Le difese: le password

Password complesse

- Lettere minuscole, maiuscole, numeri
- Simboli @ $ % * §
- Simboli particolari: Alt+123 { - Alt+125 } – Alt + 135ç
- Caratteri unicode € , #, ¬ »

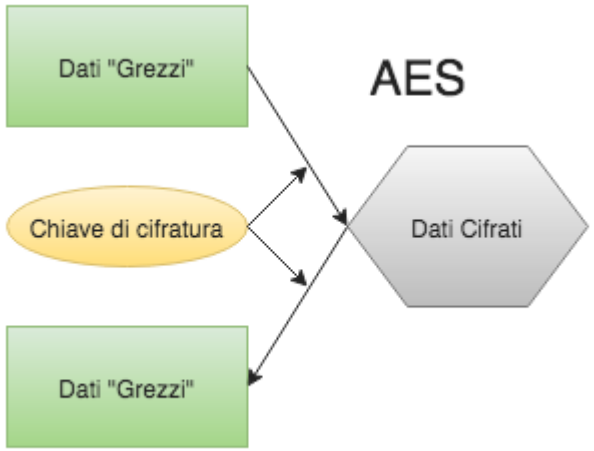
Efficacia della password:

Usare lettere e simboli appositamente creati di una frase: Voglio comprare 14 dischi

Voglio compra@re 14 $ischi -> Vc@14$chY

Le difese: la cifratura

In termini molto semplici, la cifratura è una modalità di conversione del testo (file) originale in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale.



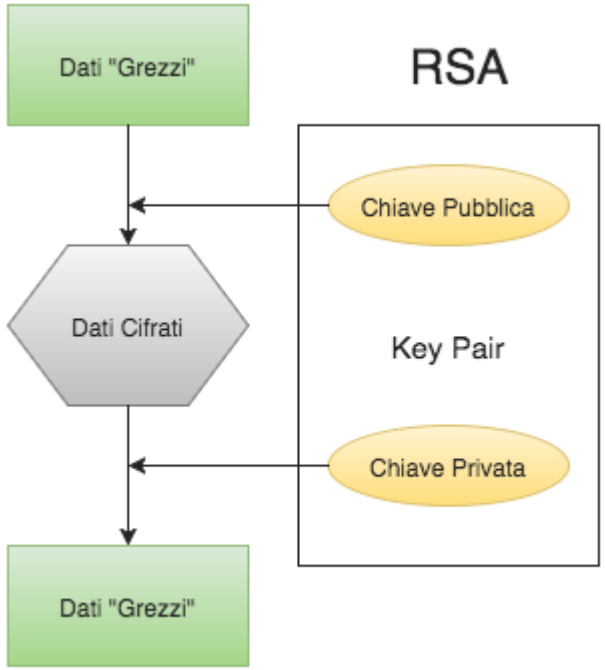
Con algoritmi crittografici si intendono tutti quei processi e procedure finalizzati ad ottenere un dato “offuscato” in modo da non essere comprensibile/intelligibile da persone non autorizzate a leggerlo.

Questa tipologia di algoritmi si basa sull’uso di chiavi di cifratura dette simmetriche che permettono di cifrare e decifrare dati utilizzando la medesima chiave crittografica. Un esempio è AES (Advanced Encryption Standard),

Le difese: la cifratura

Algoritmi Asimmetrici

Gli algoritmi asimmetrici si distinguono dai precedenti per l'utilizzo di due chiavi crittografiche distinte, dette pubblica e privata, per effettuare le operazioni di cifratura e decifratura. Il nome deriva dal metodo con il quale le due chiavi devono essere utilizzate. La chiave pubblica viene liberamente scambiata, mentre la chiave privata rimane a conoscenza solo di coloro che devono poter leggere i dati o i messaggi scambiati. In questo caso l'esempio per eccellenza è RSA, uno standard di fatto nella sicurezza riguardante la trasmissione di dati: è infatti largamente utilizzato per cifrare le comunicazioni che avvengono tra client e server.



Le difese: sicurezza perimetrale

UTM

UTM è l'acronimo di Unified Threat Management, ovvero l'unione di tutte le tecnologie informatiche dedite ad individuare, gestire ed annullare le minacce di attacco informatico rivolte ad organizzazioni aziendali singole o con reti aziendali estese e distribuite, con utenti remoti, sedi periferiche o data center remoti. Le tecnologie UTM puntano a rilevare e correggere ogni potenziale breccia del sistema informatico aziendale con l'obiettivo di prevenire e proteggere le informazioni più critiche, i database, le applicazioni software e, soprattutto, la continuità operativa aziendale

Le difese: sicurezza perimetrale

UTM

Le tecnologie che compongono le soluzioni UTM generalmente sono:

- Firewall / VPN
- Application Control
- Intrusion Detection System (IDS) e Intrusion Prevention System (IPS)
- Web Filtering (Proxy)
- WAN Optimization (bilanciamento)
- Wireless Access Point
- Endpoint Protection

SOLUZIONE ALL-IN-ONE: bene ma non troppo. Perché?

Le difese: sicurezza perimetrale

2017 GARTNER MAGIC QUADRANT FOR UTM

Gartner Inc. è una società per azioni multinazionale leader mondiale nella consulenza strategica, ricerca e analisi nel campo dell'Information Technology con oltre 60.000 clienti nel mondo. L'attività principale consiste nel supportare le decisioni di investimento dei suoi clienti attraverso ricerca, consulenza, benchmarking, eventi e notizie

Le difese: Virtual Private Network

VPN acronimo di Virtual Private Network o reti private virtuali

Il funzionamento delle VPN si basa su un tunnel virtuale tra il nostro computer e un server sicuro di proprietà dell'azienda. Tutto il traffico che effettuiamo passa in modo cifrato dal computer al server.

Utile, ad esempio, per collegare in modo sicuro un computer alla rete aziendale per attività come condivisione di file o utilizzo di applicazioni. Il computer è virtualmente collegato alla rete aziendale e lavora come se fosse fisicamente in azienda. E' possibile creare delle regole sofisticate di instradamento dalla rete VPN e la rete aziendale

Conformità al nuovo regolamento

Cosa devo fare? (1/2)

GDPR	Cosa fare
Art. 32 - [..] 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.	• Cifratura dei dati e/o partizioni e/o dishi a livello client (PDL) e server; • Centralizzazione degli utenti, ACL, architetture virtualizzate o in HA, disaster recovery; • Implementare una politica di backup e ripristino dei dati; • Implementare procedure e audit per le verifiche dei sistemi, simulare incidenti fisici e tecnici, pen test, documentare;
Art. 33 - In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo entro 72 ore […] 3. La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi […] b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.	Tutti i sistemi di difesa illustrati in precedenza (firewall, IDS, IPS, antivirus, ecc prevedendo degli strumenti di analisi in tempo reale e analisi storiche. Ad ognuno di essi è affidato il compito di proteggere il sistema ed è un tassello fondamentale della sicurezza.

Articoli: 32, 33 del GDPR

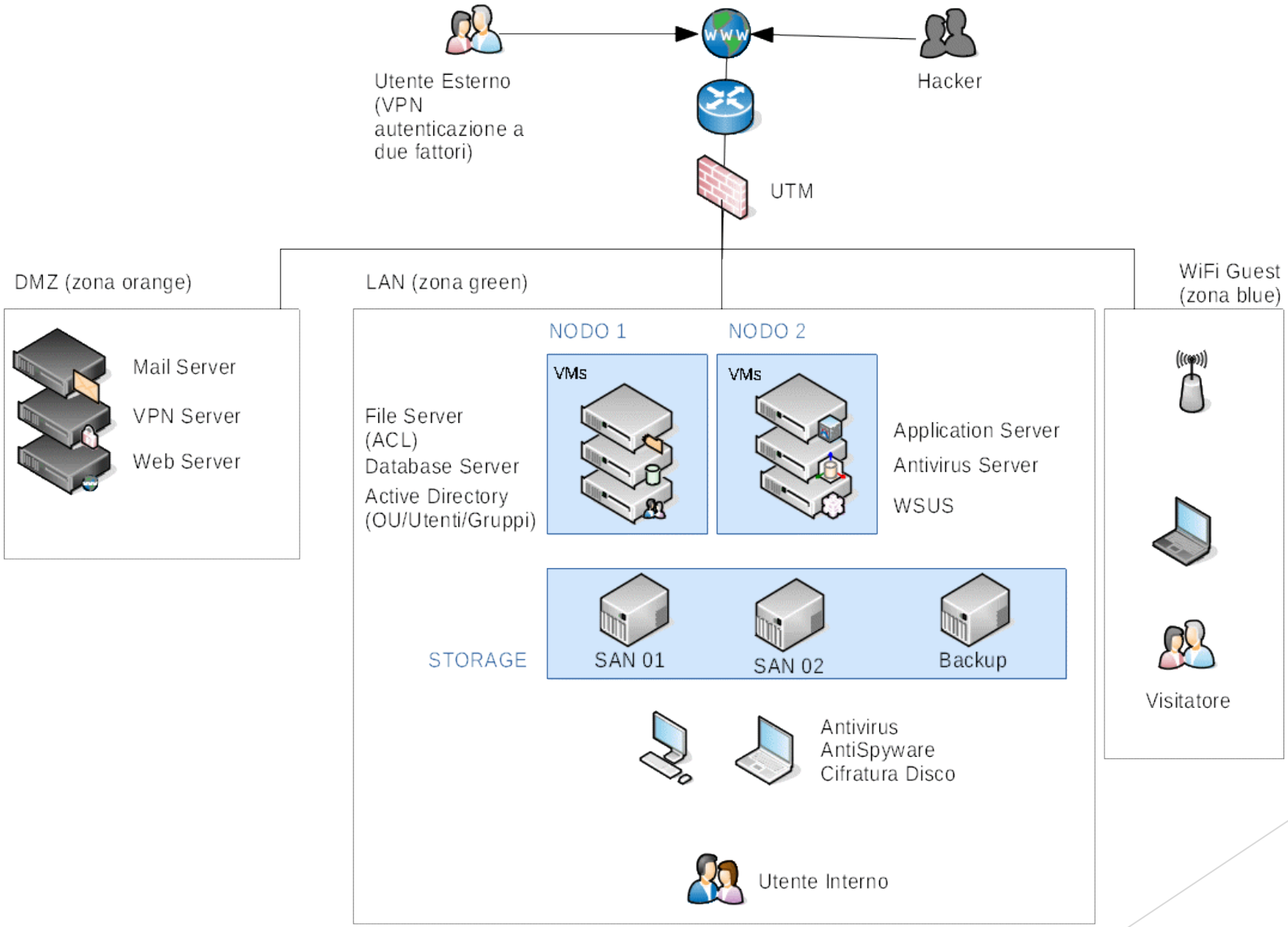
Cosa devo fare? (2/2)

GDPR	Cosa fare
Art. 35 – Analisi di impatto Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali […]	In estrema sintesi la DPIA (Data protection impact assessment) consiste in una valutazione preliminare (fatta dallo stesso titolare) degli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.
Art. 39 – Compiti del DPO Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: […] b) sorvegliare l'osservanza del presente regolamento […] c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; […]	Implementare un sistema di monitoring delle rete e infrastrutture per le verifiche in tempo reale delle risorse, utilizzo di dashboard e report per in controllo delle criticità;

Articoli: 35, 39 del GDPR

Conclusioni

Caso di studio



Domande e risposte

Siamo a vostra disposizione…