DATA BREACH:

PREVENIRE E' MEGLIO CHE CURARE

14 maggio 2021

Relatore: Col. Marco Menegazzo

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

N.S.T.P.F.T.

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE
GUARDIA DI FINANZA

DIPENDENZA GERARCHICA

UNITA' SPECIALI

AUTORITÀ DI RIFERIMENTO

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

PROTOCOLLO D'INTESA TRA AUTORITA' GARANTE E GUARDIA DI FINANZA

31 MARZO 2021

GRUPPO PRIVACY

- Gestione dei rapporti con l'Autorità Garante
- Esecuzione di ispezioni su delega dell'Autorità Garante
- Partecipazione ad ispezioni congiunte con l'Autorità Garante nonché con le Autorità di controllo di altri Stati membri (art. 62 GDPR)
- Reperimento di dati e informazioni da segnalare all'Autorità
- Sviluppo di attività progettuali in sinergia con i Reparti territoriali del Corpo

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2020 (DIS, AISE e AISI)

L'analisi degli attacchi cibernetici rilevanti per la sicurezza nazionale raccolti dall'Intelligence ha fatto emergere un generale incremento delle aggressioni (+20%), che hanno riguardato per lo più, i sistemi IT di soggetti pubblici (83%, un incremento di 10 punti percentuali rispetto al 2019) in particolare le Amministrazioni locali (48%, valore in aumento di oltre 30 punti percentuali rispetto all'anno precedente), unitamente ai Ministeri titolari di funzioni critiche (+ 2% nel confronto anno su anno).

Invece, le azioni digitali ostili perpetrate nei confronti dei soggetti privati hanno interessato prevalentemente il settore bancario (11%, in aumento di 4 punti percentuali rispetto al 2019), quello farmaceutico/sanitario (7%, in più rispetto allo scorso anno) e dei servizi IT (11%, dato pressoché stabile).

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

DATA BREACH

IL QUADRO

Attacchi cyber a tema covid, è boom: ecco i più pericolosi

Home > Malware e attacchi hacker

Condividi questo articolo

Phishing che sfrutta l'attesa del vaccino covid. Dati a rischio negli apparecchi di monitoraggio pazienti. Videoconferenze sempre nel mirino del cyber crime. Ecco una rassegna degli allarmi più gravi, alla luce di numerosi studi e rapporti

26 Ago 2020

Marco Falconi
Site Reliability Engineer

IL CASO

Donna morta per colpa di ransomware: la Sanità non cyber-sicura uccide

Home > Malware e attacchi hacker > Ransomware

Condividi questo articolo

Succede in Germania, per il blocco informatico dell'ospedale universitario di Duesseldorf. Bloccati 30 server interni, il 10 settembre, sfruttando una vulnerabilità dei gateway Citrix, denominata CVE-2019-19871. Già Wannacry aveva aumentato il tasso di mortalità connessa. Ecco perché avere ospedali cyber sicuri è vitale

18 Set 2020

L'ANALISI TECNICA

Alien, il malware che infetta le app Android e svuota i conti correnti delle vittime

Home > Malware e attacchi hacker

Condividi questo articolo

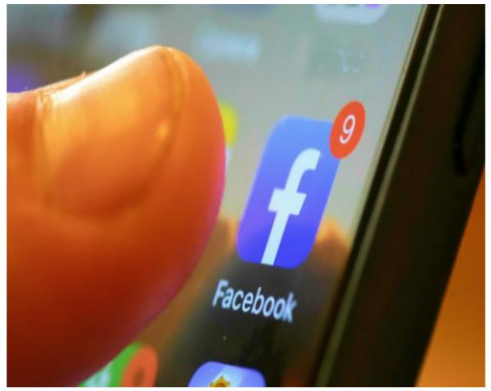
Si chiama Alien un nuovo banking trojan per Android molto insidioso che consente di sottrarre le credenziali da 226 app e agire da remoto sul device della vittima in modo del tutto indisturbato. Ecco tutti i dettagli

02 Ott 2020

Alessia Valentini
Giornalista, Cybersecurity Consultant e Advisor

il Fatto Quotidiano

Facebook, rubati e diffusi i dati di 36 milioni di italiani. Garante della Privacy: "Social fornisca un servizio per verificare il furto"



CRONACA | 11 aprile 2021, 15:03

Attacco informatico all'Agenzia territoriale per la casa di Torino: chiesto un riscatto di 700mila dollari

La Atc ha presentato denuncia alla polizia postale, dopo aver risposto alla mail degli hacker per denunciare che il loro è stato un attacco "contro tutte le 30mila famiglie delle case popolari". Il sistema è al momento bloccato

Tecnologia

Hacker bucano Ho Mobile, ecco cosa devono fare i 2 milioni di clienti a rischio

Giuseppe Mauro — 4 Gennaio 2021

Allarme privacy e rischio truffe per 500 milioni di utenti di Linkedin: dati personali dei profili in vendita online su un forum di hacker

Flash News Martedì, 06 Aprile 2021 21:16

Un cyber attacco ha violato il parlamento della Norvegia

Violate le caselle di posta elettronica dei dipendenti e di alcuni parlamentari. Anche una delle principali aziende pubbliche ha avuto disservizi con le email. Indagini in corso

Lo Storting, parlamento norvegese è stato vittima di un cyberattacco (Photo by Sigrid Harms/picture alliance via Getty Images)

ENISA: 10 PRINCIPALI TREND DEL CYBERCRIME

1. L'area o meglio la superficie di potenziali cyberattacchi continua ad espandersi con l'avvicinarsi di una nuova fase della trasformazione digitale
2. Ci sarà una nuova normalità sociale ed economica dopo la pandemia COVID-19 ancora più dipendente da un cyberspazio sicuro e affidabile
3. L'utilizzo di piattaforme di social media in attacchi mirati è una tendenza seria e raggiunge diversi domini e tipi di minacce
4. Attacchi mirati e persistenti su dati di alto valore (ad es. Proprietà intellettuale e segreti di stato) vengono pianificati ed eseguiti meticolosamente da attori sponsorizzati dallo stato
5. Gli attacchi distribuiti in modo massiccio con una breve durata e un ampio impatto vengono utilizzati con molteplici obiettivi come il furto di credenziali
6. La motivazione alla base della maggior parte degli attacchi informatici resta ancora quella finanziaria
7. Il ransomware rimane sempre diffuso con conseguenze costose per molte organizzazioni
8. Ancora molti incidenti di sicurezza informatica passano inosservati o richiedono molto tempo per essere rilevati
9. Con una maggiore automazione della sicurezza, le organizzazioni investiranno di più nella preparazione utilizzando la Cyber Threat Intelligence
10. Il numero di vittime di phishing continua a crescere poiché sfrutta la dimensione umana che è l'anello più debole

ENISA 2020 - SCENARIO DELLE MINACCE

Il direttore esecutivo dell'Agenzia dell'UE per la sicurezza informatica, Juhan Lepassaar, ha dichiarato: "Le tecniche di sicurezza informatica sono parte integrante per soddisfare gli obblighi di protezione dei dati e consentono agli utenti di godere appieno dei loro diritti fondamentali alla protezione dei dati personali e alla privacy".

IL BUSINESS DEI DATI

4 Lunedì 26 Ottobre 2020 PRIVACY ItaliaOggi7

Credenziali, follower e informazioni sanitarie mercificati nell'area oscura della rete

Dati sotto assedio nel dark web Con danni per 6 mila mld $

Pagine a cura
DI ANTONIO CICCIA MESSINA

Nel web bazar si vendono e si comprano carte di credito, credenziali bancarie, passaporti. E non solo. Se si vuole commissionare un attacco internet si può scegliere il livello di efficacia distruttiva: il listino contempla aree geografiche preferite e ci sono opzioni per i vari portafogli.

Però qualcuno può essere interessato a dati sanitari e anche in questo caso non è un problema: nel web oscuro si trova anche questo. Oppure, ancora, si può desiderare di avere un pacchetto completo di una identità da spendere nelle relazioni sul web e c'è solo l'imbarazzo della scelta.

Tutto questo si trova nel «dark web» (per distinguerlo

Come scoprire se sono stato hackerato

Controlli	Strumenti utili
Attivare un alert sul proprio nome, sul proprio cellulare, sulla propria email, in modo che non appena dovesse comparire uno dei tre elementi online nel clear web saremmo i primi a esserne informati	Google Alert TalkWalker Alert (molto veloce per trovare informazioni sui social network) https://pastebin.com (necessario autenticarsi)
Controlli sul dark web	https://ahmia.fi/
Verificare se il tuo account mail è mai stato vittima di un breach	https://haveibeenpwned.com/
Verificare se siamo vittime di attacco cyber, eseguire la ricerca tramite indicazione della mail, nome e cognome e addirittura indirizzo fisico	https://dehashed.com/
In caso rilevi il breach del tuo account segnala anche parte della password ad esso associata	https://ghostproject.fr

del trattamento di rispettare i principi generali del trattamento e di osservare la privacy quale impostazione predefinita dei propri strumenti (privacy by default) e di porsi il problema del rispetto della privacy fin dalla progettazione della sua attività (privacy by design). Quanto ai principi, l'articolo 5 del Gdpr stabilisce che il trattamento deve essere corretto, oltre che lecito. Questo significa che bisogna rispettare anche requisiti di etica e moralità delle operazioni che si compiono. Sono canoni che assumono un particolare rilievo quando si parla di dati estratti a mezzo di tecniche in grado di rilevare l'impronta del cervello. Il medesimo articolo 5 impone che i trattamenti rispondano a criteri di sicurezza.

È indispensabile che imprese e pubbliche ammini-

CLEAR E DARK WEB

IL RUOLO CHIAVE

Autorità

Titolare

Interessati

SICUREZZA NAZIONALE

ATTIVITÀ ISPETTIVA I SEM. 2021

* Data breach

Trattamenti di dati biometrici per il riconoscimento facciale anche mediante sistemi di videosorveglianza

Trattamenti di dati personali effettuati da «data broker»

Trattamenti di dati personali nel settore della c.d. «videosorveglianza domestica» e nel settore dei sistemi audio/video applicati ai giochi (c.d. giocattoli connessi)

Trattamenti di dati personali effettuati da società rientranti nel settore denominato «Food Delivery»

* Presente anche nelle deliberazioni del I e II semestre 2020

ART. 5 - PRINCIPI E DIRITTI

ARTICOLO 5
Principi applicabili al trattamento dei dati personali

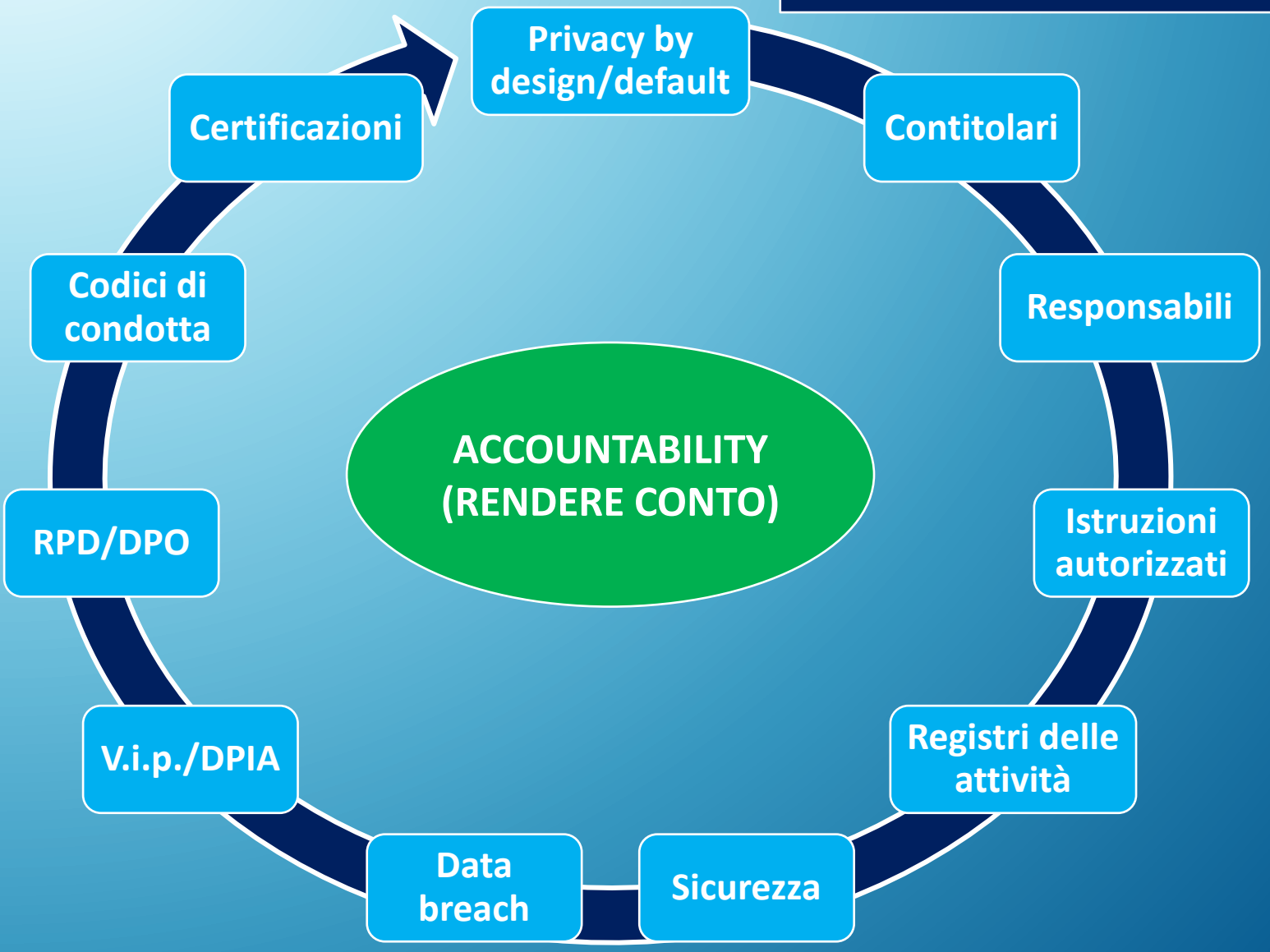
1. I dati personali sono: (C39)

(…)

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

(…)

LA COMPLIANCE



Per il GDPR deve essere dimostrata la sostanza degli adempimenti non il rispetto formale. Non basta aver adempiuto alle richieste normative, ma occorre essere in grado di DIMOSTRARLO.

Il titolare del trattamento mette in atto <u>misure tecniche ed organizzative adeguate</u> per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento (art. 24)

ARTICOLO 25
Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (C75-C78)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

(…)

ARTICOLO 28
Responsabile del trattamento (C81)

(…)

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

(…)

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

(…)

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

(…)

ARTICOLO 29
Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (C81)

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

ARTICOLO 30
Registri delle attività di trattamento (C82)

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

(…)

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

(…)

ARTICOLO 32
Sicurezza del trattamento (C83)

1. 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.

ARTICOLO 32
Sicurezza del trattamento (C83)

2. 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.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

TOP 10: PRINCIPALI SANZIONI

TITOLARE	NAZIONE	SANZIONE [€]	VIOLAZIONE
GOOGLE INC.	FRANCIA	50,000,000	Base giuridica insufficiente per l'elaborazione dei dati
H&M HENNES & MAURITZ ONLINE SHOP A.B. & CO. KG	GERMANIA	35,258,708	Base giuridica insufficiente per l'elaborazione dei dati
TIM (operatore di telecomunicazioni)	ITALIA	27,800,000	Base giuridica insufficiente per l'elaborazione dei dati
BRITISH AIRWAYS	REGNO UNITO	22,046,000	Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni
MARRIOTT INTERNATIONAL, INC	REGNO UNITO	20,450,000	Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni
WIND TRE S.P.A.	ITALIA	16,700,000	Base giuridica insufficiente per l'elaborazione dei dati
VODAFONE ITALIA S.P.A.	ITALIA	12,251,601	Base giuridica insufficiente per l'elaborazione dei dati Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni
NOTEBOOKSBILLIGER.DE	GERMANIA	10,400,000	Base giuridica insufficiente per l'elaborazione dei dati
ENI GAS E LUCE	ITALIA	8,500,000	Base giuridica insufficiente per l'elaborazione dei dati
VODAFONE ESPAÑA, S.A.U.	SPAGNA	8,150,000	Insufficiente adempimento dei diritti degli interessati

FONTE: https://www.enforcementtracker.com/

"Da un grande potere derivano grandi responsabilità"

Cit. Ben Parker - dal film Spider-Man

GRAZIE PER L'ATTENZIONE