G.D.P.R. Parte Terza

Regolamento generale sulla protezione dei dati personali

G.D.P.R.

Le tipologie di violazioni di dati personali

Analisi dei rischi

Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come **la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque trattati.**

Ciò può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).

La violazione dei dati personali può essere suddivisa in tre categorie (**R.I.D.**):

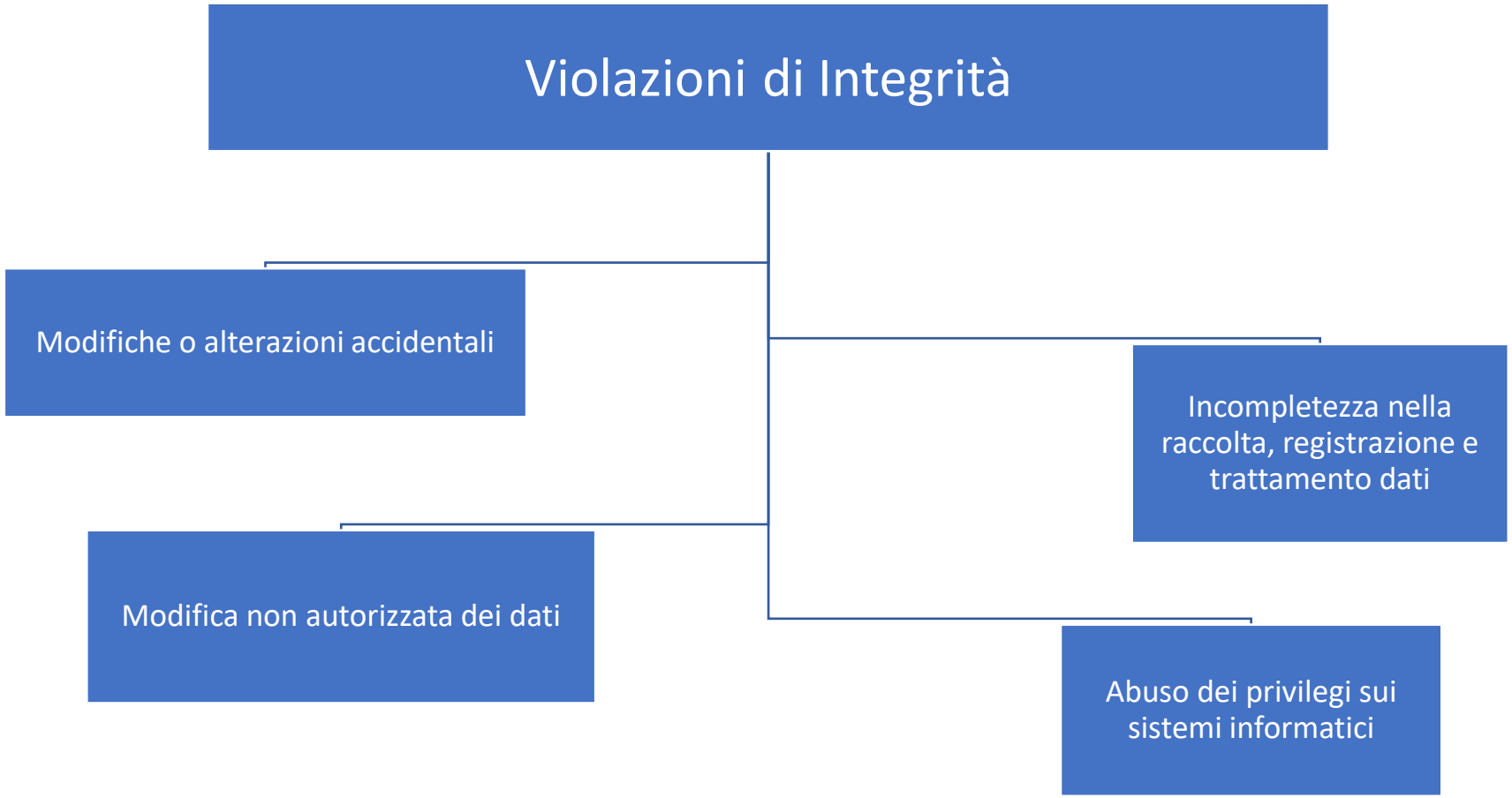
a) Violazioni di **Riservatezza**

b) Violazioni di **Integrità**

c) Violazioni di **Disponibilità**

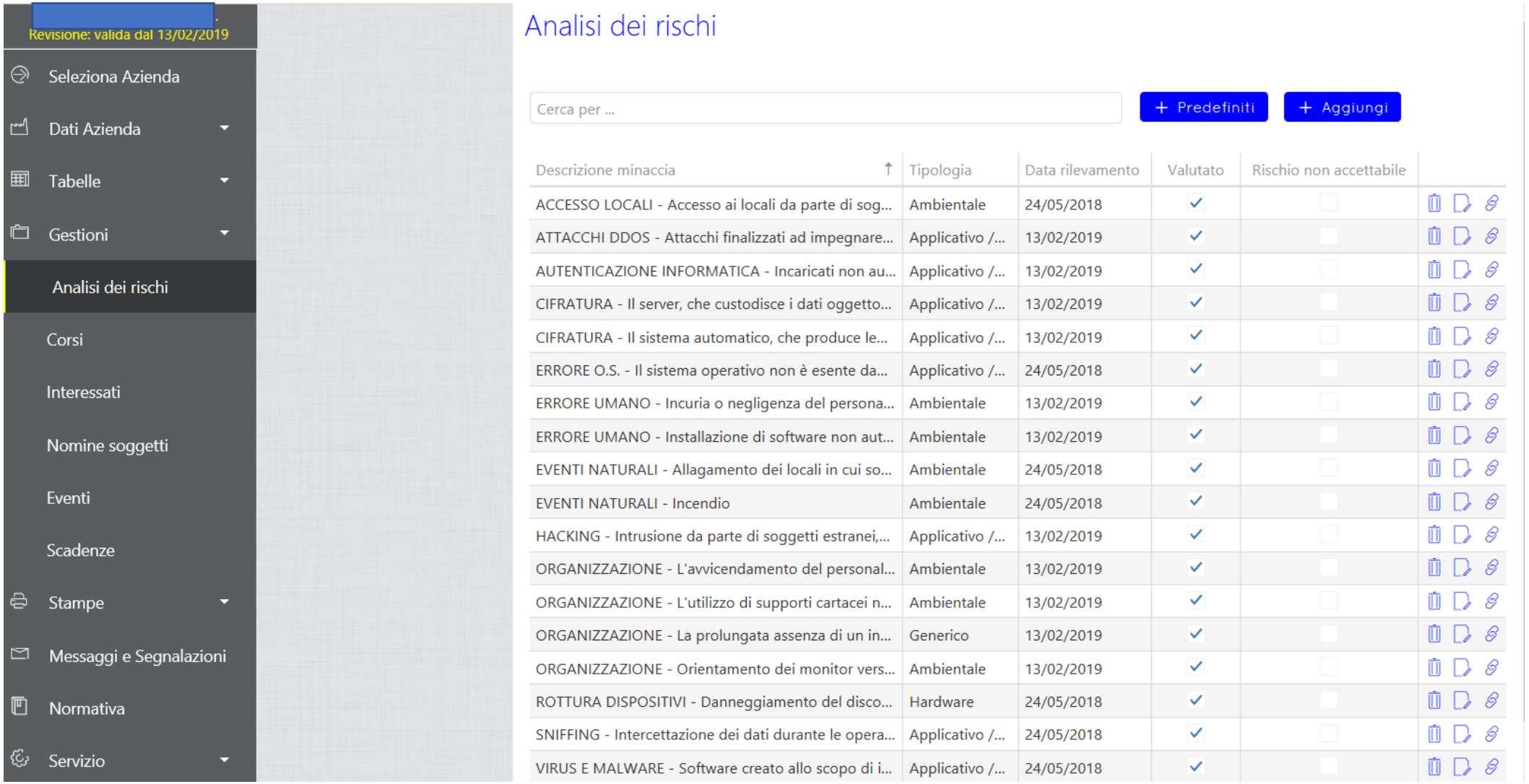
Analisi dei rischi

Analisi dei rischi



Analisi dei rischi

Analisi dei rischi



Tipologie di attacco informatico accertate

a) “man in the middle” o “ man in the mail “.

Terminologia nata per identificare tutti quegli attacchi, dall’intercettazione del traffico di rete al furto di credenziali, nei quali l’attaccante si inserisce tra due o più soggetti che stanno legittimamente comunicando.

In sostanza l’attaccante riesce ad impossessarsi dell’identità di un fornitore abituale e convince il cliente ad effettuare un bonifico su conti correnti diversi da quelli abituali.

Il mezzo utilizzo abitualmente per mettere a segno l’attacco è l’email con la tecnica dello “spear phishing”. L’attaccante, dopo aver raccolto con inganno informazioni sui rapporti abituali tra azienda cliente e proprio fornitore, invia una mail all’ignaro cliente fingendosi di essere il fornitore.

Con una scusa qualsiasi convince il cliente ad effettuare i “soliti” pagamenti su un conto corrente diverso da quello memorizzato in anagrafica.

I clienti raggirati inviano volontariamente del denaro all’attaccante, convinti di liquidare uno dei propri fornitori.

Gli hacker ritoccano l'Iban nelle email, truffe online per milioni di euro

Privacy & Società Venerdì, 28 Settembre 2018 12:21

Una mail con un falso Iban in modo da intascare milioni di euro. Si tratta di fatture e documenti ineccepibili, nessun linguaggio sospetto o mittente con nomi sconosciuti. Nella posta elettronica arrivano documenti di transazioni e spese vere, dove viene indicato l' Iban su cui versare i soldi per saldare i propri acquisti. Ed è questo l'unico dato taroccato. Più che polpette 'avvelenatè, le mail inviate dai nuovi hacker truffatori sono mail 'ritoccatè, tanto quanto basta per intascare milioni di euro.

L'inganno del 'Business email compromisè (B.e.c.) riguarda finora centinaia di utenti italiani dall'inizio del 2018, tra cui grandi aziende nostrane truffate per centinaia di migliaia di euro. I cybercriminali, alcuni dei quali operano in Italia e sui quali da mesi sta indagando la polizia postale, hanno messo in piedi un software con il quale 'bucanò le caselle di posta elettronica aziendali e dopo aver intercettato negli elenchi le parole chiave, come «fattura» o «pagamenti», bloccano le mail inviate prima che arrivino ai destinatari.

Poi viene sostituito l'Iban di riferimento, ma all'apparenza niente sembra essere stato modificato. Dunque la mail viene recapitata come se nulla fosse cambiato, solo che stavolta c'è il numero di conto corrente dell'hacker. Quei nuovi Iban in realtà portano al bottino dei cybercriminali, spesso risalente a prestanome o conti aperti con documenti falsi. E dopo qualche giorno, alla verifica della transazione, le vittime scoprono che i soldi non sono mai arrivati a chi invece avrebbe dovuto legalmente incassarli.

Controllare se la propria email è stata violata

https://haveibeenpwned.com/

Cambiare periodicamente la password della propria email

Tipologie di attacco informatico accertate

b) “Ransomware”.

I ransomware sono virus informatici – tecnicamente “trojan” – che bloccano i documenti contenuti sui sistemi infettati e chiedono un riscatto, in genere in bitcoin. Dopo essere stato contagiato dal cryptovirus, il computer continua a funzionare ma i documenti della vittima vengono protetti tramite algoritmi di cifratura.

Al pagamento del riscatto, i criminali «promettono» di sbloccare la cifratura dei documenti rimuovendo il criptovirus.

A essere colpiti dai ransomware non sono soltanto i PC con Sistema Operativo Windows, Mac OS e Linux ma anche smartphone e persino dispositivi elettronici come Smart TV, che fanno parte della categoria IoT (Internet Of Things).

L’infezione dei ransomware si diffonde in genere tramite email di phishing, con diversi soggetti e tipologie in base alle diverse ondate di ransomware.

Misure di sicurezza adeguate (Art. 32)

NON sono più previste **MISURE MINIME** come quelle indicate tassativamente e «tipizzate» nell'Allegato B D.Lgs. 196/03

TITOLARE E RESPONSABILE DEL TRATTAMENTO

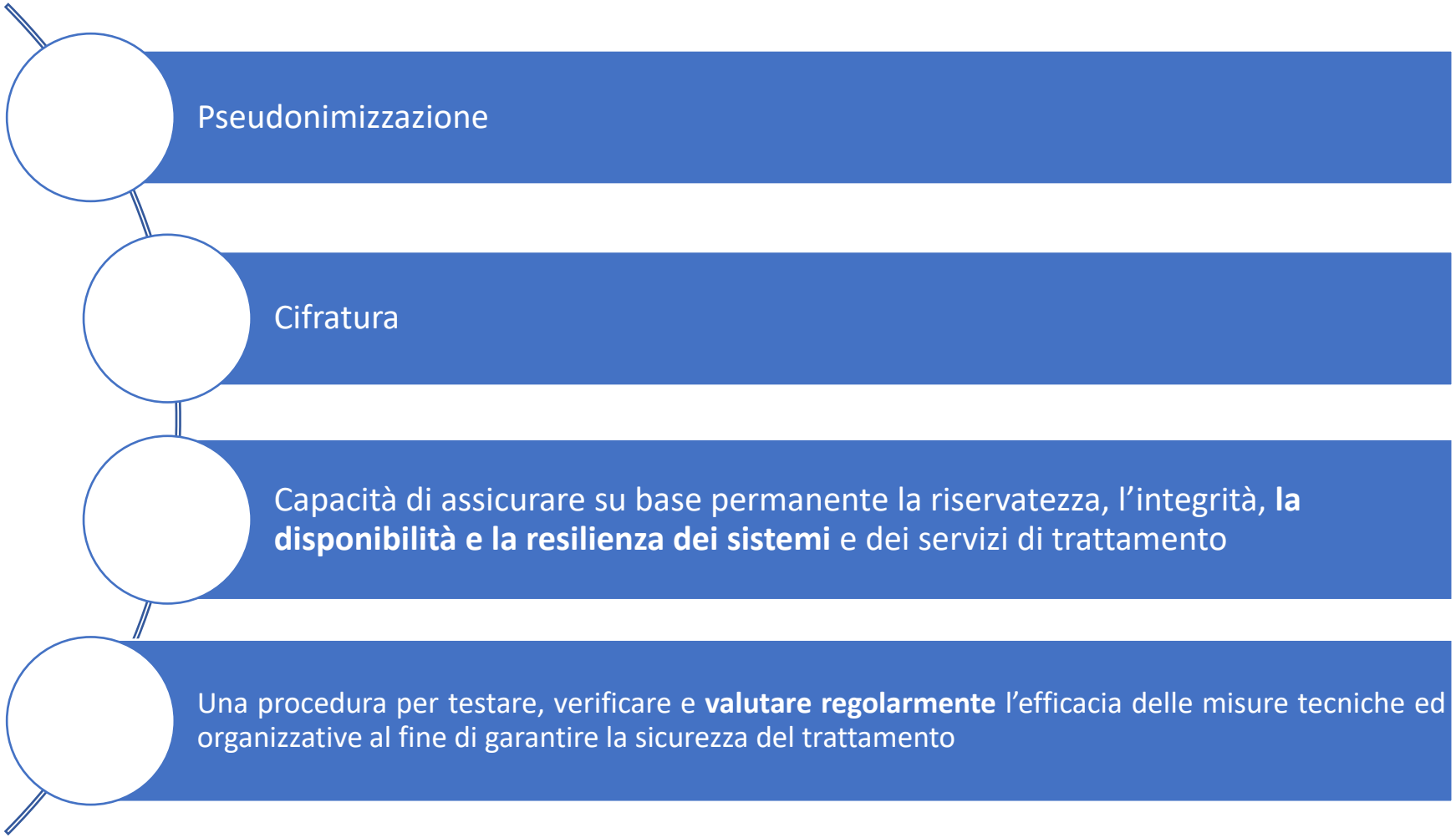
METTONO IN ATTO

MISURE TECNICHE ED ORGANIZZATIVE ADEGUATE per garantire un livello di sicurezza adeguato al rischio

tenuto conto dello stato dell'arte e dei costi di attuazione, nonché **NATURA, AMBITO, CONTESTO, FINALITA' E RISCHI**

Alcune misure di sicurezza adeguate tipizzate

Art. 32 REG. UE 679/2016



MISURE MINIME DI SICUREZZA ICT PER LE PA

Al fine di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che devono essere adottate per contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi, AgID ha provveduto ad emanare l'elenco ufficiale delle «Misure minime per la sicurezza ICT delle pubbliche amministrazioni».

Le misure si articolano su tre livelli (minime, standard, alte) prevendendo controlli di natura tecnologica, organizzativa e procedurale. Il livello minimo deve essere l'obiettivo di ogni PA indifferentemente da natura e dimensione

Fra le misure minime è previsto anche che le pubbliche amministrazioni accedano sistematicamente a servizi di early warning che consentano loro di rimanere aggiornate sulle nuove vulnerabilità di sicurezza.

AgID provvederà ad aggiornare le Misure minime tutte le volte che si renderà necessario, in funzione dell'evoluzione della minaccia cibernetica, al fine di mantenere la Pubblica Amministrazione ad un livello adeguato di protezione.

Le soluzioni di sicurezza informatica

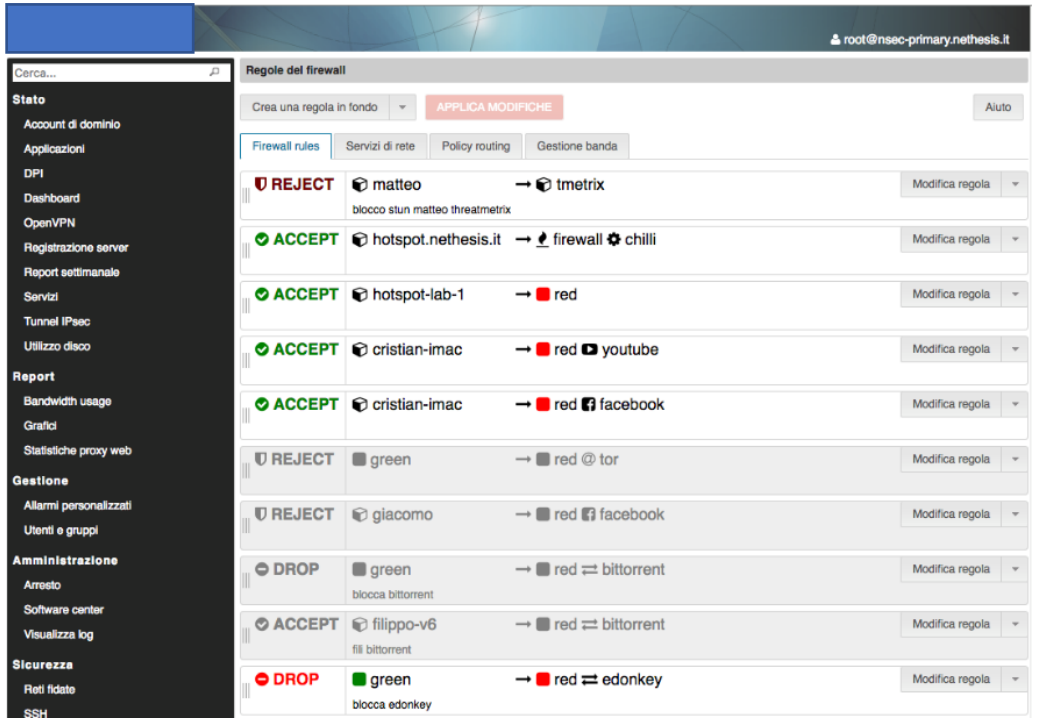
Il firewall

Strumento di interfaccia tra la rete interna e la rete internet.

- Questo dispositivo permette di filtrare il traffico in entrata e in uscita, consente di bloccare l'accesso a siti web pericolosi o ritenuti inopportuni, previene da eventuali attacchi di hacking.
- Impedisce la navigazione verso certe categorie di siti, oppure la consente solo verso certe categorie, creando vere e proprie "regole" per la navigazione e bloccando l'accesso ai contenuti indesiderati e/o pericolosi. Si potranno per esempio limitare i contenuti multimediali (radio e video in streaming) che spesso sono causa di intasamenti di banda che rallentano la navigazione di tutti gli utenti.
- Gestisce la priorità di traffico dei singoli host o gruppi di host privilegiati. Limita la banda massima consentita per la rete degli ospiti o riserva banda minima garantita per i tuoi servizi critici (SAAS, VOIP).
- Effettua collegamenti remoti (per esempio da casa o da sedi secondarie) in maniera sicura creando una VPN (Virtual Private Network), cioè una rete privata basata su protocolli di sicurezza, le cui comunicazioni in entrata ed in uscita non possono essere intercettate.

Le soluzioni di sicurezza informatica

Il firewall



Il monitor della rete controlla tutto il traffico che attraversa il firewall consentendo di individuare l'utilizzo della banda e il tipo di traffico effettuato dai vari device aziendali. Tramite tabelle e grafici viene mostrato in tempo reale l'utilizzo della banda, consentendo all'amministratore di individuare sia gli host più attivi che il tipo di traffico effettuato.

Produce una reportistica accurata permettendo di risalire all'indirizzo IP da cui proviene l'attacco, sapere a chi è assegnato o capire la tipologia della "tentata intrusione". Questi dati vengono archiviati e possono essere esportati per eventuali indagini.

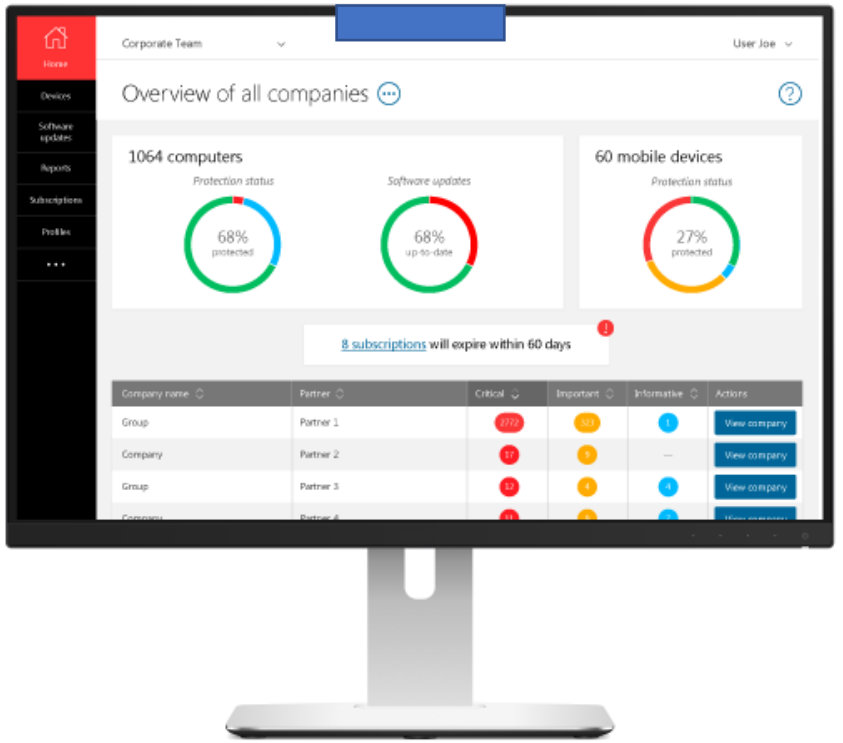
Attraverso una serie di tabelle e grafici, l'amministratore di rete può analizzare lo stato dei servizi, la configurazione e l'utilizzo delle risorse hardware del sistema, intervenendo tempestivamente (anche da remoto) in caso di necessità.

Le soluzioni di sicurezza informatica

La suite antivirus

Attraverso una console di gestione in cloud, viene monitorato lo stato di efficienza del sistema con verifica degli aggiornamenti, report sulle infezioni, gestione in remoto delle scansioni.

- Il portale di gestione fornisce una panoramica completa sullo stato della sicurezza dell'intero ambiente. Sono inclusi dispositivi su cui è stato eseguito il root, aggiornamenti di sicurezza mancanti e lo stato delle funzioni di sicurezza, come la scansione in tempo reale.
- Si può monitorare il numero di infezioni bloccate e prestare maggiore attenzione ai dispositivi che subiscono più attacchi. Si può impostare avvisi automatici via e-mail in modo da mettere in primo piano specifici parametri di infezioni.
- Fanno parte della soluzione endpoint funzionalità di protezione durante la navigazione web, filtro antispam, protezione predittiva e gestione automatica delle patch.



Le soluzioni di sicurezza informatica

La scansione delle vulnerabilità

Permette di identificare e gestire le minacce sia interne sia esterne, creare report sui rischi e assicurare la conformità alle normative attuali (per esempio la conformità PCI e GDPR). Offre visibilità sullo shadow IT - per mappare l'intera superficie d'attacco e rispondere alle vulnerabilità critiche associate alle cyber minacce.

- Mappa la superficie d'attacco con la scansione di rete e porte.
- Scansiona sistemi e applicazioni web per identificare vulnerabilità conosciute.
- Gestisce centralmente le vulnerabilità, le documenta e crea avvisi.
- Assicura la conformità con le normative attuali e future per ridurre il rischio di perdita di dati

1. Executive summary

Based on the selected scan targets and the below described summary report configuration the overall security level[1] for the systems in scope of the assessment is: **Low**.

1.1. Scope

The following 10 hosts have been scanned.

Name	Target	Findings (Changes in parenthesis)		
		High	Medium	Low
support.company.com	12.23.34.45	100	220	-
login.company.com	12.23.34.45	90	150	-
Cisco ASA Firewall	12.23.34.45	53	21	-
WordPress Blog	12.23.34.45	18	71	-
www.company.com	12.23.34.45	18	71	-
Apache web server	12.23.34.45	18	68	-
HP ProCurve	12.23.34.45	1	1	-
Splunk	12.23.34.45	0	1	-
ProFTPD	12.23.34.45	0	0	-
Unknown	12.23.34.45	0	0	-

1.2. Current system health

1.2.1. Top 10 most vulnerable targets

Platform Scan			
Target	Findings		
	High	Medium	Low
support.company.com	100	220	0
login.company.com	100	220	0
Cisco ASA Firewall	53	21	0
WordPress Blog	18	71	0

1.2.2. SSL/TLS maturity evaluation

SSL/TLS implementation issues	Affected hosts
SSL certificate is not valid	8
SSL certificate uses SHA1 signature	8
SSL3 POODLE vulnerability	6
OpenSSL Heartbleed Information Disclosure Vulnerability	4

1.2.3. Top 3 most frequent high/medium risk vulnerabilities

Platform Scan	
Vulnerability instance	Affected hosts
Apache HTTP Server Byterange Filter Denial of Service Vulnerability	9
Apache HTTP Server before 2.4.5 Unspecified Vulnerability	9
Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x DOS or buffer overflow	9
Apache HTTP Server Scoreboard Local Security Bypass Vulnerability	9
Apache HTTP Server Bad Request Error Documents Information Disclosure Vulnerability	9
Apache HTTP Server mod_proxy_balancer DoS Vulnerability	9

1.2.4. Scan group health

Scan group name	Affected hosts sorted by security		
Internet facing assets	308 (31%)	673 (68%)	0 (0%)

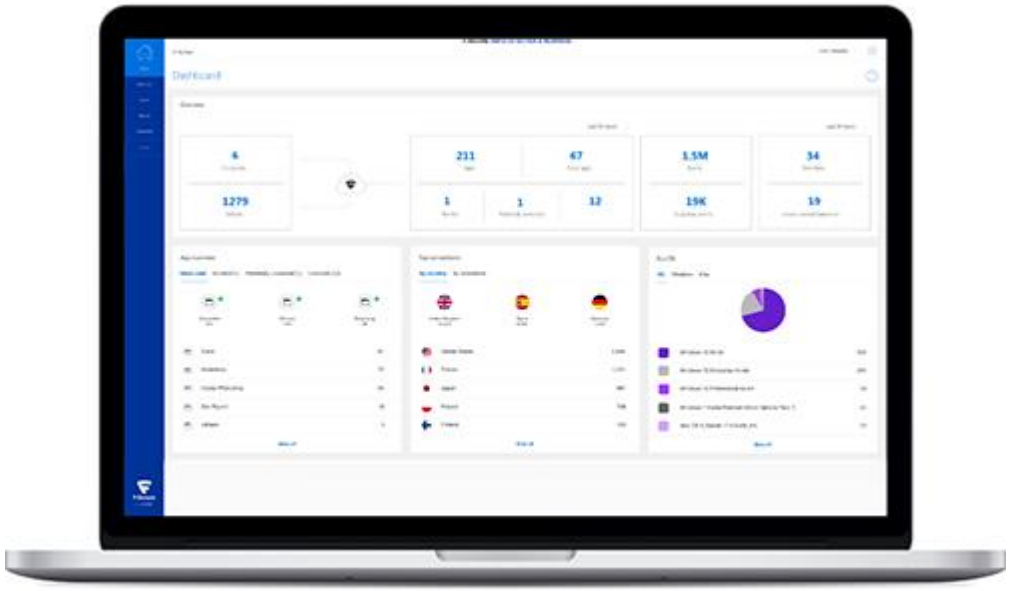
Le soluzioni di sicurezza informatica

Software di rilevamento e risposta EDR)

Soluzione di sicurezza informatica rivolta a proteggere la propria rete da minacce avanzate, violazioni ed intrusioni che causano la perdita o il furto di dati, attraverso tecniche sofisticate (APT) che non permettono la rilevazione con le tradizionali misure di protezione (ad es. antivirus e firewall).

L'agent viene installato su ogni pc della rete, client o server, ed identifica attività sospette, raccogliendo e correlando **eventi comportamentali** legati all'utilizzo della postazione di lavoro. Tutti gli eventi vengono raccolti ed analizzati da un sistema di **intelligenza artificiale**, filtrati in avvisi di vario livello di criticità e forniti, attraverso un pannello di controllo, al reparto IT per le successive misure di contrasto.

Questo permette di **rilevare e bloccare** rapidamente gli attacchi mirati, ed essere in regola con la rilevazione dei **data breaches** prevista dal Reg. UE 679/2016.



G.D.P.R.

Il Disciplinare relative all’utilizzo dei dati personali

Misure organizzative

Disciplinare relativo all'utilizzo dei dati

Regole di condotta ed obblighi dei collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica redatto anche ai sensi del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei.

Misure organizzative

Premessa

Ogni dato personale di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita del titolare del trattamento.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta

Misure di sicurezza

Ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dallo studio, nonché quelle che in futuro verranno comunicate.

Sistemi informatici

Per ogni incaricato viene creata una "credenziale di autenticazione" che consente l'accesso ai dati, attraverso una procedura di autenticazione

Tale parola chiave deve essere modificata al primo utilizzo autonomamente da parte sua, evitando quindi che la stessa sia conosciuta e comunicata a terzi e tenendo presenti le seguenti istruzioni:

- la parola chiave deve avere una lunghezza minima di otto caratteri (o, se minore, comunque utilizzi la lunghezza massima permessa dal sistema);
- la parola chiave non deve essere facilmente riconducibile alla sua persona.

Essa non va comunicata ad altri incaricati; deve essere variata autonomamente da lei stesso con periodicità trimestrale in caso di trattamento di dati c.d. sensibili e/o giudiziari.

La postazione informatica non va lasciata incustodita; tutti i supporti magnetici utilizzati vanno riposti negli archivi; i supporti non più utilizzati possono essere eliminati solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili.

Sistemi informatici

Non possono essere installati né utilizzati programmi per elaboratore non autorizzati dal notaio né privi di licenza che ne legittimi l'uso. Gli strumenti informatici e telematici messi a disposizione (a seconda dei casi: personal computer, software, navigazione su internet, e-mail, ecc.) costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate.

All'incaricato è vietato:

- La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
- Installare alcun software di cui l'organizzazione non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione.
- Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
- Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa del titolare del trattamento.
- Accedere ed utilizzare informazioni non autorizzate o non necessarie per le mansioni svolte.

Internet

È vietata la navigazione nei siti che possono rivelare le opinioni politiche, religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati particolari previsti dal GDPR.

È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato.

È vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet.

È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare.

È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo la denominazione del titolare, salvo autorizzazione.

È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.

È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'organizzazione stessa.

Posta elettronica

In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.

Avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

Inoltre:

È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa.

È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.

È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

Antivirus

L’incaricato deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

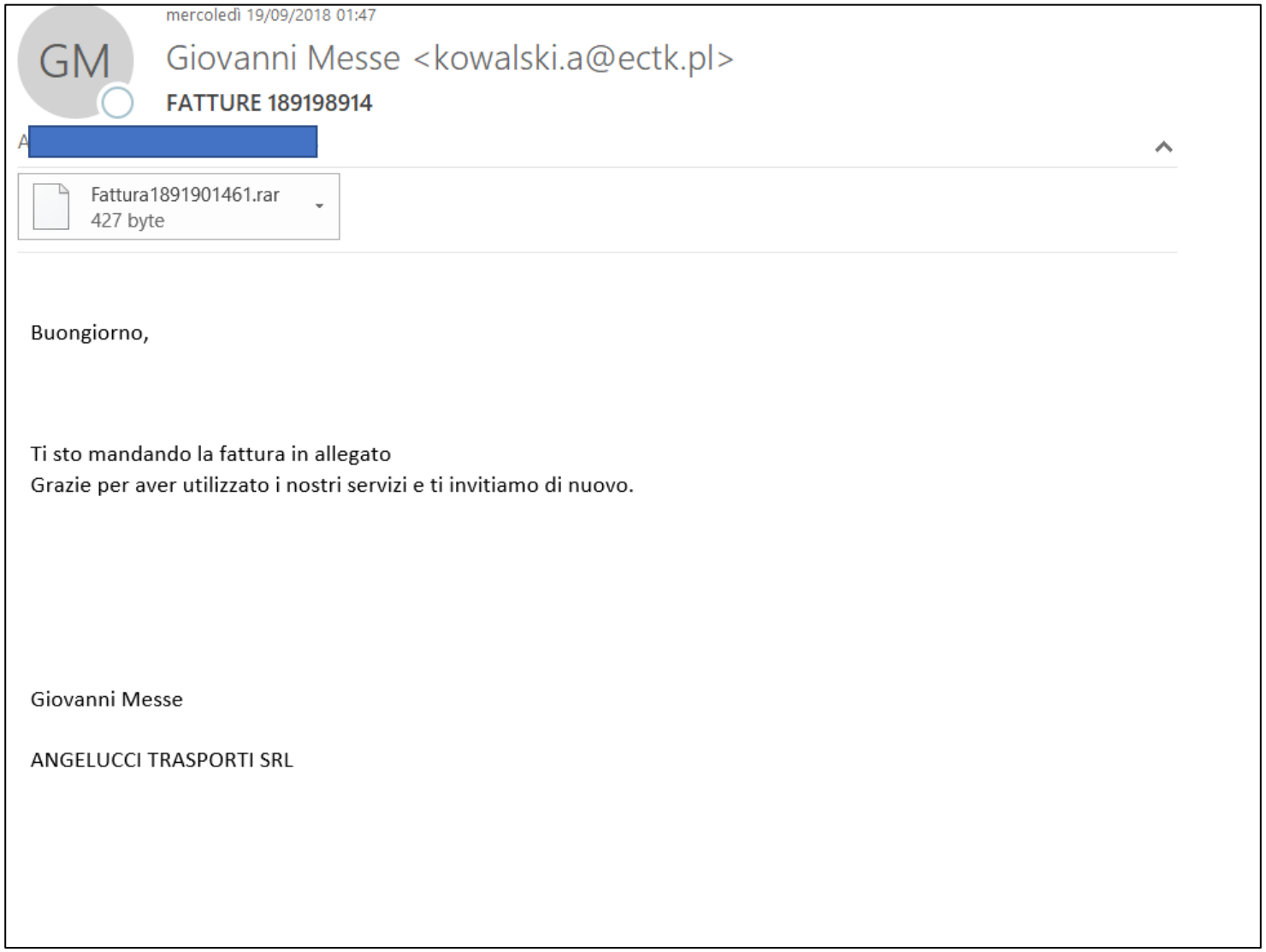
- Comunicare al Titolare ogni anomalia o malfunzionamento del sistema antivirus;
- Comunicare al Titolare eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all’incaricato:

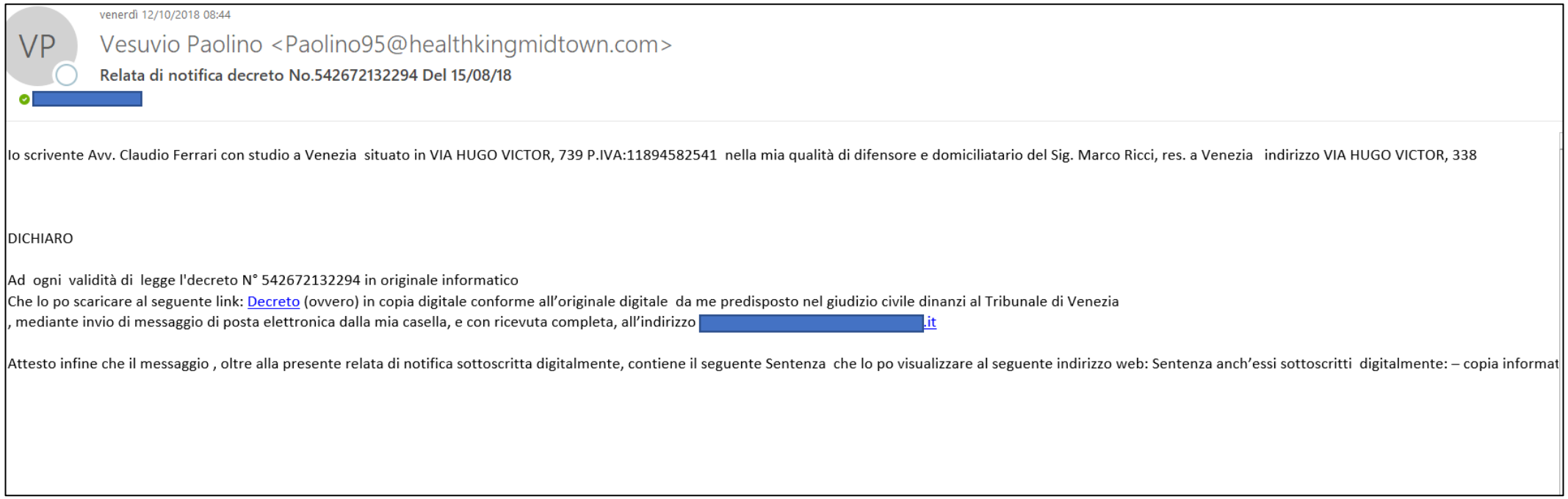
- È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
- È vietato ostacolare l'azione dell'antivirus aziendale;
- È vietato disattivare l’antivirus senza l’autorizzazione espressa del titolare anche e soprattutto nel caso sia richiesto per l’installazione di software sul computer;
- È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

Chi di voi aprirebbe l’allegato di questa mail?



..od il link nella mail?



venerdì 12/10/2018 08:44

VP

Vesuvio Paolino <Paolino95@healthkingmidtown.com>

Relata di notifica decreto No.542672132294 Del 15/08/18

[redacted]

Io scrivente Avv. Claudio Ferrari con studio a Venezia situato in VIA HUGO VICTOR, 739 P.IVA:11894582541 nella mia qualità di difensore e domiciliatario del Sig. Marco Ricci, res. a Venezia indirizzo VIA HUGO VICTOR, 338

DICHIARO

Ad ogni validità di legge l'decreto N° 542672132294 in originale informatico
Che lo po scaricare al seguente link: Decreto (ovvero) in copia digitale conforme all'originale digitale da me predisposto nel giudizio civile dinanzi al Tribunale di Venezia
, mediante invio di messaggio di posta elettronica dalla mia casella, e con ricevuta completa, all'indirizzo [redacted].it

Attesto infine che il messaggio , oltre alla presente relata di notifica sottoscritta digitalmente, contiene il seguente Sentenza che lo po visualizzare al seguente indirizzo web: Sentenza anch'essi sottoscritti digitalmente: – copia informat

Trattamenti cartacei

Le indicazioni relative alla privacy suggeriscono di collocare i fascicoli in locali in cui non abbiano accesso diretto né clienti né terzi, quindi non nell'ingresso, nella sala d'aspetto o nei corridoi.

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'organizzazione.

È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

G.D.P.R.

Le procedure

Data breach

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare all' Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore e senza ingiustificato ritardo,** ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Pertanto la notifica all'autorità non è obbligatoria ma è subordinata alla valutazione del rischio per gli interessati, e tale valutazione spetta al titolare.

Se il rischio è elevato si dovranno informare, **senza ingiustificato** ritardo tutti gli interessati.

I contenuti della notifica all'Autorità e agli interessati sono indicati agli **art. 33 e 34 del regolamento**.

Guida del Garante Privacy

Raccomandazione

Data breach

Tutti i titolari del trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e provvedimenti adottati (art. 33.5).

Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Definizione di violazione di dati personali

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione;
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o di archivi contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

PRIMA FASE DEL DATA BREACH

Individuazione del tipo di violazione e comunicazione immediata al Titolare del trattamento.

Chiunque rilevi una qualsiasi violazione o compromissione di dati personali ne dà immediata comunicazione al Titolare del trattamento, mediante la compilazione del *Modulo di comunicazione Data Breach al titolare del trattamento*, specificando i dati coinvolti e descrivendo l'evento secondo la seguente tipologia:

Violazione di riservatezza (divulgazione o accesso a dati personali non autorizzato o accidentale);

Violazione di integrità (alterazione di dati personali non autorizzata o accidentale);

Violazione di disponibilità (perdita, inaccessibilità, distruzione, accidentale o non autorizzata, di dati personali).

Modulo di comunicazione Data Breach al titolare del trattamento

Comunicazione di Data Breach al Titolare	**Note**
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Nome della persona che ha riferito della violazione:	
Tipologia della violazione dei dati personali:	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	

SECONDA FASE DEL DATA BREACH

Avvio dell'azione correttiva per gestire tecnicamente la violazione e per ripristinare, se necessario, tempestivamente la disponibilità e l'accesso dei dati personali.

TERZA FASE DEL DATA BREACH

Analisi dei rischi conseguenti alla violazione. In particolare, si deve valutare se la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche.

QUARTA FASE DEL DATA BREACH

In caso di assenza di rischi per i dati personali

Procedere alla registrazione della violazione nell'apposito Registro delle violazioni

In caso di presenza di rischi per i dati personali

Entro 72 ore dalla scoperta della violazione, procedere alla notifica al Garante della Privacy, tramite apposito modulo scaricabile dal sito: https://www.garanteprivacy.it/documents/10160/2052659/Modello+segnalazione+data+breach.pdf

In caso di presenza di un rischio elevato

Entro 72 ore inviare la notifica al Garante della Privacy;

senza ingiustificato ritardo inviare la notifica agli interessati per consentire loro l'adozione di ogni precauzione per ridurre al minimo il potenziale danno derivante dalla violazione dei dati;

gestire i riscontri da parte degli interessati.

Non è richiesta la comunicazione all'interessato se:

- sono state messe in atto tutte le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

- sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

- la comunicazione richiederebbe **sforzi sproporzionati:** in tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

REGISTRO DELLE VIOLAZIONI

Data violaz.	*Natura violaz.*	*Categoria interessati*	*Categoria dati personali*	*Numero dai dati personali coinvolti*	*Conseguenze violazione*	*Contromisure adottate*	*Notifica Garante*	*Notifica interessati*