OPEN IT S.R.L.

OPEN SOFTWARE OPEN MIND

GDPR, alcuni passi per abituarsi ad un metodo

GDPR...

Il concetto di sicurezza informatica nell'ottica del **GDPR**

Sicurezza informatica...

La sicurezza nell' ambito informatico equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

Il centro nevralgico...

Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

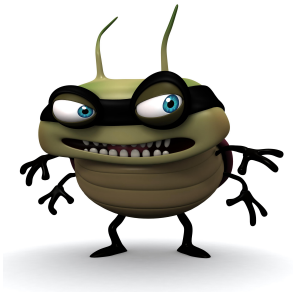
Gli attacchi...

Con il GDPR il concetto di sicurezza informatica ha assunto un significato più moderno e attuale tenendo in considerazione gli attacchi ed incidenti di natura „telematica/informatica“. La recrudescenza del fenomeno sta diventando preoccupante.

Cosa interessa?

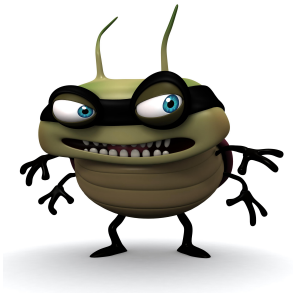
Negli ultimi tempi si è assistito ad una rapida evoluzione della minaccia “cibernetica” che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

Pericolo 1...

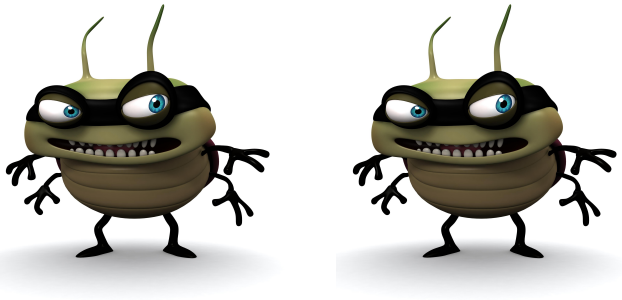


I pericoli:

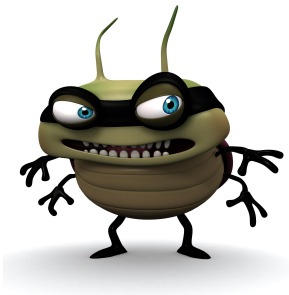
la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati;



Pericolo 2...



il secondo pericolo deriva dal fatto che il primo obiettivo venga perseguito attraverso tecniche che permettono di nascondere l‘attività illecita, in modo da non destare sospetti



L‘anello debole...

La combinazione dei due fattori precedenti impone di fare **attenzione** alle attività degli utenti che consideriamo, giustamente, fidati.

(*Indipendentemente da firewall, antivirus, difesa perimetrale e verifiche hardware*)

L‘anello debole...

Gli attacchi non sono quasi mai diretti ma si avvalgono anche dell‘aiuto inconsapevole (o consapevole) degli utenti stessi.

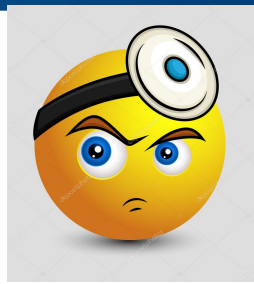
Prevenzione...

Prevenzione è la parola d‘ordine ma è insufficiente se non vengono utilizzati strumenti di rilevazione del danno che diano risposte in tempi brevi.

Prevenzione...

Più sarà tardiva l‘individuazione del danno e minore sarà la possibilità di tornare alle condizioni normali in tempi ragionevoli.

Vulnerabilità...



Individua i punti deboli!!!

Prima soluzione...

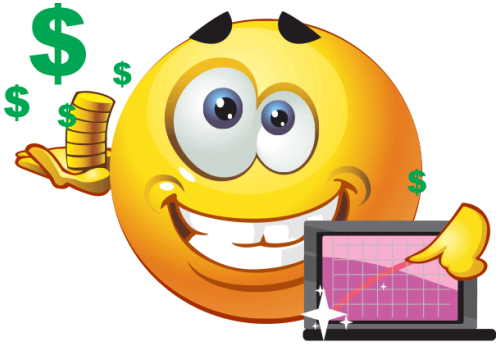
Elimina i punti deboli sia dal punto di vista informatico che procedurale e non perdere di vista il fattore umano ché sarà quello a metterti in crisi.

Violazione al GDPR...

Il titolare del trattamento o il responsabile del trattamento deve valutare anche il rischio informatico

Violazione al GDPR...

rischio di danni economici (rischi diretti)



Violazione al GDPR...

reputazione (rischi indiretti) derivanti dall'uso della tecnologia
rischi impliciti nella tecnologia
rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali

Violazione al GDPR...

In particolare i processi operativi automatici possono essere:

- **danneggiamento di hardware e software;**
- **errori nell'esecuzione delle operazioni nei sistemi;**
- **malfunzionamento dei sistemi;**
- **programmi indesiderati**

Soluzioni possibili...

Per ovviare a tali rischi vanno individuate le corrette soluzioni senza dimenticare la cifrature dei dati in caso di particolari problematiche.

I moderni sistemi operativi hanno soluzioni che prevedono anche tali escamotage!

Valutazione 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 elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Titolare e responsabile trattamento...

Il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Titolare e responsabile trattamento...

In caso di trattamento

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Disaster recovery...

Backup: una parola Bantù che significa:

avresti potuto salvarti il c…uore!

Disaster recovery...

Il regolamento prevede un piano per l'analisi del rischio di inoperatività del sistema informatico e la messa a punto di un piano di emergenza che permetta di riprendere il normale lavoro anche in modalità provvisoria o con servizio elaborazione dati alternativo.

Disaster recovery...

Backup: non lo deve controllare il tuo fornitore, i dati sono tuoi. TU sei tenuto a controllare i TUOI e i MIEI dati se te li ho affidati. Ricordalo!!!

Tranquillità...

I Dati sono una parte importante anche della tua vita oltre che del tuo lavoro: Curali!

Tranquillità...

Grazie per l'attenzione!
Diaolin, alias Giuliano Natali!

diaolin@diaolin.com