GDPR 2018 25 MAGGIO POCHI GIORNI ALLA SCADENZA

GDPR 2018 25 MAGGIO POCHI GIORNI ALLA SCADENZA

0 settimane, 5 giorni, poche ore e pochi minuti alla scadenza dei 2 anni per l’adeguamento al G.D.P.R

Vi sono molteplici ragioni per cui si rischia di essere in ritardo con il completamento delle attività di conformità GDPR.

Avete veramente voglia di rischiare?

Caronni srl puo’ offrirti la consulenza e le soluzioni hardware e software di cui hai bisogno per essere compliance GDPR.

Alcuni nostri clienti hanno già aderito all’offerta apprezzando le competenze degli esperti di cui Caronni si avvale per poter proporre la soluzione su misura al fine di rispondere alla normativa.

Il sistema dei nostri servizi prevede anche l’acceso a una piattaforma cloud a supporto del trattamento dei dati

sensibili all’interno dell’azienda e dello studio, per tenere costantemente aggiornata la documentazione G.D.P.R e la generazione di tutti i documenti previsti dalla normativa.

Riconosceremo ai nostri clienti le migliori condizioni economiche per l’acquisto dei prodotti e dei servizi necessari alla Compliance.

In qualità di Vs. fornitore di servizi informatici , conoscendo in dettaglio la vostra infrastruttura di IT possiamo offrirvi un’offerta economica puntuale e dettagliata su quelli che dovranno essere necessariamente gli aggiornamenti hardware e software da effettuare con piu’ urgenza.

Siamo a vostra disposizione per qualsiasi chiarimento e richiesta.

Caronni srl – Direzione commerciale. 0362 559383 – 1

Le moderne stampanti o copiatrici multifunzione

Le moderne stampanti o copiatrici multifunzione.

La stampante multifunzione comunemente chiamata: “multifunzione” o stampante “all-in-one” è una tipologia di periferica che si contraddistingue per il fatto di integrare in un unico blocco hardware **almeno tre diverse periferiche**: una stampante, una fotocopiatrice e

uno scanner.

La stampante multifunzione è quindi sempre in grado di eseguire altre due operazioni oltre alla stampa: la scansione di superfici piane e la produzione di fotocopie.

Inoltre possono eventualmente essere **integrate** nella stampante multifunzione **anche altre periferich**e, come ad esempio un modem o una scheda di rete. In tale caso la stampante multifunzione è in grado di eseguire operazioni come ad esempio l'invio di facsimili ed e-mail da scansione. Se integrata ad un software di archiviazione puo' diventare d'aiuto a servizi documentali centralizzati in azienda.

Operazioni svolte dalla stampante multifunzione

Le moderne stampanti o copiatrici multifunzione quando gestite dal computer (ormai il 99% delle situazioni) possono svolgere le seguenti operazioni:

- stampare,
- scansionare documenti,
- fotocopiare,
- faxare (solo se la stampante multifunzione è dotata di modem),
- inviare immagini per posta elettronica (solo se la stampante multifunzione è dotata di scheda di rete).

Ambiti di utilizzo della stampante multifunzione

La stampante multifunzione è molto apprezzata in ambito Small Office Home Office. In particolare in tale ambito sono apprezzati i costi inferiori da sostenere (rispetto all'acquisto e alla gestione di più apparecchi distinti), oltre alla riduzione degli ingombri richiesti.

Vantaggi e svantaggi della stampante multifunzione

Le moderne stampanti o copiatrici multifunzione hanno il **vantaggio**, rispetto alle stampanti tradizionali, di fornire **funzionalità aggiuntive** senza richiedere l'acquisto di strumenti separati, come uno scanner d'immagini, una fotocopiatrice o un fax.

Le stampanti multifunzione hanno in genere un **costo** superiore rispetto a quello di una normale stampante ma **inferiore rispetto alla somma delle macchine separate**. In genere si considera che possano avere prestazioni inferiori rispetto all'apparato specifico con il vantaggio però di una riduzione dell'ingombro fisico e/o dei consumi[senza fonte] e del prezzo d'acquisto.

Altro grande **vantaggio** delle stampanti multifunzioni stà nel **minor costo relativo al volume di stampe aziendale**. Infatti se lo stesso volume viene sviluppato distribuito su diverse periferiche, magari anche di tipologia diversa, il costo a parità di volume ne risulta anche triplicato, costi nscosti aggiuntivo sono anche il dover gestire tipologie di ricambi "toner" tra loro diversi. Lo svantaggio relativo al costi di acquisto oggi è praticamente annullato dalla diffusione di forme di **noleggio operativo** in cui l'azienda non è proprietaria dello strumento ma, attraverso un canone di norma molto basso in relazione al valore della multifunzione, usufruisce da subito senza pesanti esborsi di uno strumento ottimo e a volte anche positivamente surdimensionato rispetto alle proprie necessità e con il canone che in un unica cove, comprende anche la manutenzione e i pezzi di ricambio della stessa.

I **vantaggi** sono quindi **di tipo economico** , **funzionale ed amministrativo** nel senso che non ci si dovrà occupare nel tempo di gestione di contratti di manutenzione, acquisti di toner , gestione degli ammortamenti etc.

Lo "**svantaggio**" è che dovrete fare qualche passo in piu' nell'ufficio che si traduce però **in vantaggio** alla vs. **salute;** già perchè muoversi fa bene ma fa ancora meglio il non avere nel proprio ufficio uno strumento , anche se

corredato da filtri a norma, che puo’ comunque generare polveri di certo non positive sulla nostra salute.

Aggiornamento sulla sicurezza del 03/05/2019

Aggiornamento sulla sicurezza del 03/05/2019

Consigli, avvisi, novità sui rischi connessi alla sicurezza informatica.

1.GandCrab 2.1: in diffusione un nuovo ransomware tramite email di spam.

Scoperta in the wild, quindi già in diffusione contro utenti reali, una nuova variante del noto ransomware GandCrab. Questo ransomware, ormai alla seconda versione, bersaglia sopratutto paesi anglofoni e scandinavi.

Viene diffuso principalmente attraverso email dannose: solitamente l’oggetto delle email fa riferimento a invio di documenti importanti, ricevute di pagamenti, ordini di vario tipo, ticket e buoni sconto ecc… Una tecnica pensata proprio per ingannare l’utente e convincerlo a scaricare l’archivio compresso. La criptazione avviene usando l’algoritmo di cifratura RSA, che non altera tutto il file, ma solo una parte, quella sufficiente a renderlo inutilizzabile dall’utente. Ogni file viene criptato utilizzando una chiave unica, il che rende molto molto difficile procedere alla decriptazione dei file stessi. I file criptati non vengono rinominati, ma il ransomware ne modifica l’estensione in .CRAB.

2.FacexWorm: il malware in diffusione su Facebook Messenger e Chrome

Gli utenti di Google Chrome, Facebook e tutti coloro che utilizzano cirptovalute devono prestare attenzione ad una nuova tipologia di malware chiamata FacexWorm: questo malware è specializzato nel furto di password, nel furto di criptovalute dai fondi delle vittime, nell'esecuzione di script per il mining e per un elevato livello di spam contro gli utenti Facebook.

La catena di infezione inizia solitamente quando un utente riceve link attraverso messaggi di spam su Facebook Messenger. Il clic su questo link conduce a una pagina web che imita Youtube: tramite alcuni avvisi questa falsa pagina Youtube prova a convincere gli utenti a installare una fantomatica estensione collegata a Youtube per Google Chrome. Questa estensione ha numerose funzioni dannose, ma la più grave è quella per la quale l'estensione aggiunge del codice al browser degli utenti per rubare le credenziali dai form di login. Le credenziali raccolte vengono quindi inviate ai server controllati dai cyber attaccanti.

3.Una analisi dell'infezione Dharma ransomware – Quick Heal Security Labs

Abbiamo notato una impennata improvvisa delle individuazioni del ransomware Dharma sui pc dei nostri utenti. Il Ransomware Dharma non è affatto nuovo e anzi, la prima versione, distinguibile dall'estensione ".dharma" è perfino risolvibile. Non lo è però la seconda versione in distribuzione, quella attuale, che cripta i file in ".arrow".

Il ransomware Dharma è diffuso principalmente attraverso due vettori: la porta RDP e altre forme di vettori. Il Remote Desktop Protocol (RDP) eseguito sulla porta 3389, viene solitamente bersagliato da un attacco di brute-forcing. Come risultato l'attaccante può riuscire ad ottenere l'accesso all'account Admin. Una volta ottenuti i privilegi di admin, l'attaccante ha la capacità di eseguire qualsiasi tipo di attacco: in questo caso installa il ransomware Dharma. Nel secondo caso invece non conoscevamo la fonte di infezione, ma, una volta iniziato lo studio dell'infezione, abbiamo subito notato interessanti voci aggiunte al registro della vittima. Stiamo parlando di voci di registro aggiunte dagli attaccanti.

4. Necurs: la più grande SPAM botnet usa una tecnica che bypassa gli antivirus per diffondere malware.

Necurs è indubbiamente la botnet più estesa al mondo, composta da milioni di dispositivi infetti finiti sotto il suo controllo: ne abbiamo parlato spesso come “centro nevralgico” di attacchi spam, phishing e per la distribuzione di exploit e a malware di ogni tipo. Proprio in questi giorni ha subito un update: ha migliorato il proprio “equipaggiamento” e usa attualmente una nuova tecnica per infettare le vittime.

Proprio in questi giorni Necurs ha subito un update: ha migliorato il proprio “equipaggiamento” e usa una nuova tecnica per infettare le vittime. Questa tecnica consiste nell’invio di una mail ad una nuova, potenziale vittima con un file allegato: questo file, una volta estratto, contiene un altro file in formato .URL. Questo è un tipico file di collegamento che apre una pagina web direttamente nel browser invece che in una location in locale. La destinazione finale di questo link è un file script remoto che scarica e esegue automaticamente il payload finale. Il perchè dell’uso dei file .URL è semplice: una catena di infezione così semplice riesce ad evitare gli scanner antimalware che analizzano ogni singola email in cerca di link dannosi o allegati compromessi.

5. Curiosità: hackerato il sito della RedBull: 2 volte! (per colpa di Drupal)

Il sito della Redbull, produttrice del famosissimo drink energizzante, è stato recentemente attaccato da un gruppo di cyber attaccanti. Non sono stati fatti cambiamenti né sostituzioni nella pagina principale del sito, ma sono solo aggiunte alcune pagine prima inesistenti. Una di queste pagine dice “hacked by Prosox”: questa breve rivendicazione è seguita da un link che conduce al profilo Twitter dell’hacker.

Stando a varie fonti, sarebbero stati attaccati oltre 30 sottodomini Redbull: le indagini hanno rivelato che è stato usato uno script CMS e l’attacco è stato distribuito usando Drupal.Drupal, un popolare CMS open source, è sotto osservazione da qualche settimana a causa delle gravi vulnerabilità riscontrate e per l’impressionante serie di attacchi che stanno bersagliando da qualche settimana i siti gestiti con Drupal. La (prima) falla di sicurezza CRITICA riscontrata, Drupalgeddon2, ha permesso una lunghissima serie di attacchi contro siti gestiti con Drupal. Solo che, risolta la prima, è arrivata la seconda falla critica…

Errori comuni nell’uso della posta elettronica

Errori comuni nell’uso della posta elettronica

Normalmente quando inviate un’email e c’è un problema, l’email vi torna indietro con anche la motivazione del perché non è stata recapitata.

I messaggi email che contengono l’oggetto **Delivery Status Notification** sono messaggi, spesso in lingua inglese, generati automaticamente dai sistemi di posta con lo scopo di informare il mittente sullo stato della email inviata, e più frequentemente del motivo per cui l’invio non è andato a buon fine.

Il nostro servizio di supporto è a disposizione, a pagamento, per supportarVi su qualsiasi problema potreste incontrare nell’utilizzo del vs. sistema di posta. Se avete necessità di supporto aprite una richiesta di intervento al nostro **sistema di supporto.**

Di seguito riportiamo gli errori comuni nell’uso della posta elettronica che vi possono aiutare a risolvere da soli molti dei problemi incontrati.

Elenco dei messaggi di errore e soluzioni possibili :

- **MAILBOX FULL**: la capienza della casella di posta alla quale abbiamo inviato il messaggio ha raggiunto il limite massimo di capienza consentito, e non è pertanto in grado di ricevere ulteriori messaggi; è necessario attendere che l'utente legga e cancelli alcuni messaggi, se il problema persiste è probabile che si tratti di un indirizzo di posta non più in uso.
- **BAD DESTINATION MAILBOX ADDRESS** o **USER UNKNOWN**: l'indirizzo di posta al quale abbiamo inviato il messaggio non esiste; controllare eventualmente di averlo digitato senza errori.
- **ROUTING SERVER FAILURE**: il dominio (sempre leggibile a destra del simbolo **@** in un indirizzo) non esiste; controllare eventualmente di aver digitato correttamente l'indirizzo email, come ad esempio *utente@libero.it* e non*utente@libro.it* .
- **RELAYING NOT ALLOWED**: siamo connessi con un provider e contemporaneamente utilizziamo nelle impostazioni del server di posta in uscita (SMTP) di un provider diverso; utilizzare per il server SMTP i parametri del provider con il quale si è connessi.
- **OTHER OR UNDEFINED PROTOCOL STATUS** o **OTHER OR UNDEFINED MAIL SYSTEM STATUS** o **OTHER OR UNDEFINED NETWORK OR ROUTING STATUS**: si tratta generalmente di un temporaneo problema remoto sulla rete o sul sistema di posta; riprovare ad inviare il messaggio in un secondo momento.
- **ACTION: FAILED**: il server di posta non è riuscito ad inoltrare il messaggio; accanto di solito è specificato uno dei motivi esaminati prima, controllare l'indirizzo del destinatario ed eventualmente inviare di nuovo il messaggio.
- **ACTION: DELIVERED**: il messaggio inviato è stato recapitato a destinazione; si può ricevere di solito se in un primo momento ci sono stati problemi o ritardi nell'invio.
- **ACTION: RELAYED**: il messaggio è stato ritrasmesso.
- **DELIVERY TIME EXPIRED**: l'invio non è andato a buon fine nonostante i ripetuti tentativi; solitamente è specificato il tempo di durata del tentativi, controllare di aver digitato correttamente l'indirizzo ed eventualmente riprovare.
- **MESSAGE TOO BIG**: il messaggio inviato non è stato accettato dalla casella di destinazione a causa delle elevate dimensioni; questa impostazione può essere di default del provider o impostata manualmente dall'utente destinatario, informare l'utente dell'allegato che gli si vuole inviare.
- **INVALID DOMAIN NAME SYNTAX**: l'indirizzo del destinatario non è stato scritto nella dovuta forma; apportare le correzioni necessarie e riprovare.

La Black List per i messaggio di posta

La Black List per i messaggi di posta

Se per caso scoprite che le vostre email non arrivano più ai destinatari e vengono respinte come sospetto SPAM, potrebbe essere che il vostro sistema di posta in uscita (in generale servizio SMTP, dominio o casella) sia stato inserito in una blacklist (Lista Nera).

Queste blacklist sono liste di indirizzi di mittenti ritenuti per qualche motivo “indesiderati” e sono mantenute da alcuni server su internet che segnalano a tutti quali sono i server SMTP/domini/casella sospettati di fare dello spam.

Se il vostro server SMTP è finito in una di queste liste, la vostra email verrà rifiutata. In genere nel messaggio di errore che torna indietro viene spiegato il motivo del mancato recapito.

Quello che succede è che il server del destinatario controlla da chi arriva l'email confrontando l'indirizzo IP del server che gliel'ha mandata con queste liste. Se l'indirizzo IP è inserito in una di queste liste, allora la posta viene rifiutata.

Di solito il server SMTP che utilizzate per spedire i messaggi in uscita è quello che vi viene fornito dal vostro provider di connessione (Alice, Tiscali, Libero, Tele2, ecc.) e per scoprirlo basterà che guardiate nel vostro programma di posta elettronica, in Account, dove è indicato "Server di posta in uscita" oppure "Server SMTP". Ad esempio per tiscali è smtp.tiscali.it.

Un altro motivo per cui è possibile che il vostro dominio o il vostro server SMTP di spedizione finisce in blacklist è perchè state facendo SPAM spesso a vostra insaputa (con il server di spedizione , il vostro dominio o una vostra mail) e di conseguenza il vs. dominio, la mail o il server SMTP viene inserito in blacklist al fine di segnalare ai destinatari di non accetttare mail da voi inviate in quanto non piu' attendibili.

Se quindi il vostro sistema di spedizione è finito in una black list occorre avviare la pratica di "delisting" ovvero la richiesta di rimozione del vostro server di spedizione dalla bleack list o dalle black list in cui è finito.

L'operazione non è complessa ma richiede delle conoscenze specifiche.

(Servizio a pagamento per aziende senza pacchetti prepagati o contratti o per servizi non previsti dal proprio piano contrattuale – Accedendo al servizio si accettano le condizioni e le relative tariffe)
