Cyber Risk Full Report

Fattori di Cyber Risk

Analizzati per **PLASTITOMAX SRL** sul dominio: **PLASTITOMAX.COM**

Numero di Domini

La piattaforma KYND ha scoperto **2** domini che sono connessi a **Plastitomax SRL**. I domini possono essere utilizzati per ospitare siti Web, così come altri servizi.

2 Domini scoperti per l'organizzazione

Sicurezza della Email

La piattaforma KYND ha verificato SPF e DMARC per **Plastitomax SRL** e ha valutato queste policy in relazione alla possibilità di spoofing delle e-mail.

@plastitomax.com può essere contraffatto

Plastitomax SRL vs aziende simili

Problemi dei certificati

42 % dei certificati sono obsoleti o diffidenti

I certificati di sicurezza sui siti Web garantiscono agli utenti che i loro dati siano al sicuro e che siano collegati al sito corretto. Se il sito Web utilizza certificati obsoleti o sospetti, gli utenti riceveranno un avviso sul proprio browser Internet e le applicazioni che utilizzano il sito potrebbero non funzionare. È necessario disporre di processi per mantenere e rinnovare i certificati del sito Web o ritirare quelli non più necessari.

In ritardo | **Indietro** | Nella media

Servizi configurati male

0 % dei tuoi servizi non sono configurati correttamente

Sebbene alcune delle infrastrutture IT debbano essere visibili pubblicamente, non necessariamente tutte lo devono essere. Database, pannelli di controllo dell'amministratore e accesso da sviluppatori devono essere limitati alle sole persone che ne hanno diritto. Quando si configurano i servizi, è importante assicurarsi che l'accesso sia limitato a coloro che lo richiedono.

In ritardo | Indietro | **Nella media**

Servizi non aggiornati

24 % dei tuoi servizi è notevolmente obsoleta

Mantenere i servizi aggiornati è essenziale per garantire una presenza online sicura. Le versioni precedenti dei servizi possono avere vulnerabilità ben note e ben visibili, che possono essere sfruttate dagli hacker per ottenere l'accesso. L'aggiornamento del software alla versione supportata più recente garantisce la protezione dei servizi da tali vulnerabilità.

In ritardo | **Indietro** | Nella media

Protezione Dominio

100 % dei tuoi domini ha problemi

Perdere il controllo di alcuni o di tutti i propri domini può comportare un rischio aziendale. Registrare domini con indirizzi e-mail individuali o dell'agenzia che ha creato il sito Web aumenta questo rischio, che potrebbe comportare la perdita di importanti aggiornamenti e scadenze, o gli hacker potrebbero individuare come bersaglio una e-mail individuale per assumere il controllo dei domini.

In ritardo | Indietro | Nella media

L'analisi dei rischi prova a identificare tutti i domini Internet registrati all'organizzazione e i servizi Internet esterni che da questi hanno origine. A causa di dati di registrazione incompleti o imprecisi, potrebbe essere collegato all'organizzazione un dominio che di fatto non è di sua proprietà, oppure potrebbe non essere identificato ogni dominio che l'organizzazione ha registrato in quanto non presente un collegamento noto o apparente. Questo potrebbe influire sull'analisi e sul report elaborato.

Da dove cominciare? Si raccomanda di verificare prima queste cinque criticità

1 Chiudere l'accesso pubblico ai database

Ci sono **1** accessi da sviluppatore aperti pubblicamente, permettendo a terzi di controllarli o installare ransomware.
L'accesso dovrebbe essere ristretto per proteggere l'accesso ai dati e servizi.

Fattori di rischio:

- public assets
- data theft
- ransomware
- security

2 Aggiungere una policy per l'email spoofing

Non c'è un record DMARC per le email di **@plastitomax.com**, rendendole vulnerabili allo spoofing.
Un record di base DMARC dovrebbe essere aggiunto per cominciare a moniotorare lo spoofing delle email. Basta inserire questo record su _dmarc.**plastitomax.com** :"v=DMARC1 p=none rua=mailto:[insertAddress]**@plastitomax.com**"

Fattori di rischio:

- phishing
- email
- financial
- reputational

3 Rivedere i dati di registrazione

plastitomax.com è stato registrato utilizzando una mail personale appartenente a **Plastitomax SRL** . Importanti comunicazione e avvisi inviate dal domain registrar, potrebbero non venire lette da dipendenti assenti o non più in azienda, inoltre le persone sono molto più soggette ad attacchi informatici. Questo rende **Plastitomax SRL** più vulnerabile ad attacchi informatici e service failure.
Questo dominio dovrebbe essere registrato utilizzando email di gruppo esempio domainadmin**@plastitomax.com**. I dati di registrazione per gli altri {numberofslds} domini di **Plastitomax SRL** dovrebbero pure essere controllati.

Fattori di rischio:

- social engineering
- lapsed processes
- control assets
- business interruption

4 Aggiornare software vulnerabile

Ci sono **3** istanze di Apache web server sull'infrastruttura di **Plastitomax SRL**, che mettono a rischio di malware & ransomware.
La version **2.4.10** di Apache ha gravi vulnerabilità che sono note, e ha bisogno di essere adeguate urgentemente.

Fattori di rischio:

- vulnerable assets
- ransomware
- malware
- business interruption

5 Aggiornare software vulnerabile

Ci sono **2** servizi vulnerabili sull'infrastruttura di **Plastitomax SRL**, che mette a rischio di malware & ransomware.
Questi servizi hanno gravi vulnerabilità che sono note, e hanno bisogno di essere adeguati urgentemente.

Fattori di rischio:

- vulnerable assets
- ransomware
- malware
- business interruption

High Risk

Colore	Dettagli	Descrizione
!	**High Risk:** 1 **Data:** 07/11/2020 **Categoria:** Dominio **Argomento:** Registrazione dominio	E' stata utilizzata una e-mail individuale di una azienda **leonardo.davinci@plastitomax.com** per registrare **webplastitomax.com**. Le notifiche critiche e gli avvisi inviati dalla società di registrazione possono essere non considerate se il dipendente è assente o se si tratta di ex dipendente. Gli individui sono anche più inclini agli attacchi informatici di social engineering. Avere un dominio registrato con una e-mail individuale rende un'organizzazione più vulnerabile agli attacchi informatici e al fallimento del servizio. Vi consigliamo di cambiare la email di registrazione del dominio **webplastitomax.com** presso **TUCOWS DOMAINS INC.**, con una email aziendale ad esempio come "domainadmin@mycompany.com" (ovviamente sostituirete con il dominio dell'email della vostra azienda).
!	**High Risk:** 2 **Data:** 07/11/2020 **Categoria:** Dominio **Argomento:** Registrazione dominio	E' stata utilizzata una e-mail individuale di una azienda **raffaello.sanzio@plastitomax.com** per registrare **plastitomax.com**. Le notifiche critiche e gli avvisi inviati dalla società di registrazione possono essere non considerate se il dipendente è assente o se si tratta di ex dipendente. Gli individui sono anche più inclini agli attacchi informatici di social engineering. Avere un dominio registrato con una e-mail individuale rende un'organizzazione più vulnerabile agli attacchi informatici e al fallimento del servizio. Vi consigliamo di cambiare la email di registrazione del dominio **plastitomax.com** presso **TUCOWS DOMAINS INC.**, con una email aziendale ad esempio come "domainadmin@mycompany.com" (ovviamente sostituirete con il dominio dell'email della vostra azienda).
!	**High Risk:** 3 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	**Apache httpd 2.2.3** è obsoleto e non è più supportato dagli sviluppatori. Questo servizio utilizza la porta **80** sull'indirizzo IP **62.149.157.166**. Il software obsoleto non è più supportato o mantenuto dai suoi sviluppatori, il che significa che i bug non saranno corretti e le vulnerabilità non saranno sanate, rendendo un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Questo servizio dovrebbe essere aggiornato con l'ultima versione. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi che richiedo l'aggiornamento dei servizi quando richiesto dai fornitori di software.
!	**High Risk:** 4 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	**Apache httpd 2.2.3** è obsoleto e non è più supportato dagli sviluppatori. Questo servizio utilizza la porta **443** sull'indirizzo IP **62.149.157.166**. Il software obsoleto non è più supportato o mantenuto dai suoi sviluppatori, il che significa che i bug non saranno corretti e le vulnerabilità non saranno sanate, rendendo un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Questo servizio dovrebbe essere aggiornato con l'ultima versione. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi che richiedo l'aggiornamento dei servizi quando richiesto dai fornitori di software.
!	**High Risk:** 5 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	**Apache httpd 2** è obsoleto e non è più supportato dagli sviluppatori. Questo servizio utilizza la porta **80** sull'indirizzo IP **91.212.167.73**. Il software obsoleto non è più supportato o mantenuto dai suoi sviluppatori, il che significa che i bug non saranno corretti e le vulnerabilità non saranno sanate, rendendo un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Questo servizio dovrebbe essere aggiornato con l'ultima versione. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi che richiedo l'aggiornamento dei servizi quando richiesto dai fornitori di software.
!	**High Risk:** 6 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	**Apache httpd 2** è obsoleto e non è più supportato dagli sviluppatori. Questo servizio utilizza la porta **443** sull'indirizzo IP **91.212.167.73**. Il software obsoleto non è più supportato o mantenuto dai suoi sviluppatori, il che significa che i bug non saranno corretti e le vulnerabilità non saranno sanate, rendendo un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Questo servizio dovrebbe essere aggiornato con l'ultima versione. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi che richiedo l'aggiornamento dei servizi quando richiesto dai fornitori di software.
!	**High Risk:** 7 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Servizio vulnerabile	Il prodotto **OpenSSH 6.7p1 Debian 5+deb8u8** presenta una vulnerabilità di sicurezza nota e critica. Questo servizio utilizza la porta **22** sull'indirizzo IP **185.6.72.90**. Perché è così importante? L'esecuzione di qualsiasi software con una vulnerabilità nota rende un'organizzazione estremamente vulnerabile agli attacchi e al fallimento del servizio. Le vulnerabilità del software appena scoperte vengono rese note pubblicamente per avvertire tutti gli utenti dei prodotti e gli sviluppatori. Purtroppo, gli hacker condividono anche strumenti e tecniche che possono essere utilizzati per sfruttare queste debolezze non appena vengono rese pubbliche. Questo servizio dovrebbe essere aggiornato con l'ultima versione, fare riferimento al sito web **OpenSSH** per ulteriori dettagli. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi di aggiornamento dei servizi quando richiesto dai fornitori di software.
!	**High Risk:** 8 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Servizio vulnerabile	Il prodotto **ProFTPD 1.3.2** presenta una vulnerabilità di sicurezza nota e critica. Questo servizio utilizza la porta **21** sull'indirizzo IP **91.212.167.73**. Perché è così importante? L'esecuzione di qualsiasi software con una vulnerabilità nota rende un'organizzazione estremamente vulnerabile agli attacchi e al fallimento del servizio. Le vulnerabilità del software appena scoperte vengono rese note pubblicamente per avvertire tutti gli utenti dei prodotti e gli sviluppatori. Purtroppo, gli hacker condividono anche strumenti e tecniche che possono essere utilizzati per sfruttare queste debolezze non appena vengono rese pubbliche. Questo servizio dovrebbe essere aggiornato con l'ultima versione, fare riferimento al sito web **ProFTPD** per ulteriori dettagli. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi di aggiornamento dei servizi quando richiesto dai fornitori di software.

High Risk: 9
Data: 07/11/2020
Categoria:
Servizio
Argomento:
Servizio vulnerabile

Il prodotto **Apache httpd 2.4.10** presenta una vulnerabilità di sicurezza nota e critica. Questo servizio utilizza la porta **443** sull'indirizzo IP **185.6.72.90**. Perché è così importante? L'esecuzione di qualsiasi software con una vulnerabilità nota rende un'organizzazione estremamente vulnerabile agli attacchi e al fallimento del servizio. Le vulnerabilità del software appena scoperte vengono rese note pubblicamente per avvertire tutti gli utenti dei prodotti e gli sviluppatori. Purtroppo, gli hacker condividono anche strumenti e tecniche che possono essere utilizzati per sfruttare queste debolezze non appena vengono rese pubbliche. Questo servizio dovrebbe essere aggiornato con l'ultima versione, fare riferimento al sito web **Apache httpd** per ulteriori dettagli. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi di aggiornamento dei servizi quando richiesto dai fornitori di software.

High Risk: 10
Data: 07/11/2020
Categoria:
Servizio
Argomento:
Servizio vulnerabile

Il prodotto **Apache httpd 2.4.10** presenta una vulnerabilità di sicurezza nota e critica. Questo servizio utilizza la porta **80** sull'indirizzo IP **185.6.72.90**. Perché è così importante? L'esecuzione di qualsiasi software con una vulnerabilità nota rende un'organizzazione estremamente vulnerabile agli attacchi e al fallimento del servizio. Le vulnerabilità del software appena scoperte vengono rese note pubblicamente per avvertire tutti gli utenti dei prodotti e gli sviluppatori. Purtroppo, gli hacker condividono anche strumenti e tecniche che possono essere utilizzati per sfruttare queste debolezze non appena vengono rese pubbliche. Questo servizio dovrebbe essere aggiornato con l'ultima versione, fare riferimento al sito web **Apache httpd** per ulteriori dettagli. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi di aggiornamento dei servizi quando richiesto dai fornitori di software.

High Risk: 11
Data: 07/11/2020
Categoria:
Servizio
Argomento:
Servizio vulnerabile

Il prodotto **Apache httpd 2.4.10** presenta una vulnerabilità di sicurezza nota e critica. Questo servizio utilizza la porta **8080** sull'indirizzo IP **185.6.72.90**. Perché è così importante? L'esecuzione di qualsiasi software con una vulnerabilità nota rende un'organizzazione estremamente vulnerabile agli attacchi e al fallimento del servizio. Le vulnerabilità del software appena scoperte vengono rese note pubblicamente per avvertire tutti gli utenti dei prodotti e gli sviluppatori. Purtroppo, gli hacker condividono anche strumenti e tecniche che possono essere utilizzati per sfruttare queste debolezze non appena vengono rese pubbliche. Questo servizio dovrebbe essere aggiornato con l'ultima versione, fare riferimento al sito web **Apache httpd** per ulteriori dettagli. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi di aggiornamento dei servizi quando richiesto dai fornitori di software.

High Risk: 12
Data: 07/11/2020
Categoria:
Servizio
Argomento:
Software non aggiornato

MySQL 5.1.34 è obsoleto e non è più supportato dagli sviluppatori. Questo servizio utilizza la porta **3306** sull'indirizzo IP **91.212.167.73**. Il software obsoleto non è più supportato o mantenuto dai suoi sviluppatori, il che significa che i bug non saranno corretti e le vulnerabilità non saranno sanate, rendendo un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Questo servizio dovrebbe essere aggiornato con l'ultima versione. Implementare una procedura per controllare regolarmente l'aggiornamento del software (ad esempio un registro di tutti i software utilizzati, dove viene utilizzato, e chi è responsabile del suo aggiornamento). Non ritardare o ignorare i messaggi che richiedo l'aggiornamento dei servizi quando richiesto dai fornitori di software.

High Risk: 13
Data: 07/11/2020
Categoria:
Servizio
Argomento:
Servizio vulnerabile

MySQL database sta attualmente utilizzando la porta **3306** sull'indirizzo IP **91.212.167.73**. Si tratta di una porta aperta che è direttamente visibile e accessibile da Internet. Perché è così importante? Una 'porta' è un punto di arrivo di comunicazione per il software in esecuzione su una rete del computer. Gli hacker, quando attaccano un'organizzazione, eseguono una 'scansione porte' sulla rete di destinazione, alla ricerca di porte 'aperte' per identificare i servizi con vulnerabilità che poi sfruttano. Avere una porta aperta rende un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Questo servizio dovrebbe essere immediatamente nascosto dietro un firewall o la porta chiusa.

High Risk: 14
Data: 07/11/2020
Categoria:
Certificato
Argomento:
Certificato di sicurezza

plastitomax.com ha un certificato auto-firmato. Se un dominio viene utilizzato per siti web o applicazioni di clienti esterni ma ha un certificato auto-firmato, i principali browser web visualizzeranno un avviso di sicurezza ai visitatori e impediranno loro di raggiungere il sito. Tutte le applicazioni che utilizzano questo dominio potrebbero non funzionare. Questo non è solo un rischio significativo per la sicurezza, ma potenzialmente dannoso per la fiducia dei vostri clienti nel vostro sito web. Generalmente, i certificati di sicurezza dovrebbero essere rilasciati da un'Autorità di Certificazione di fiducia, ma è possibile utilizzare un certificato auto-firmato solamente per i vostri siti web o le vostre applicazioni interne. Vi raccomandiamo di aggiornare il certificato di sicurezza ad uno di un'Autorità di Certificazione di fiducia per essere al sicuro.

High Risk: 15
Data: 07/11/2020
Categoria:
Certificato
Argomento:
Certificato di sicurezza

tecno.plastitomax.com ha un certificato auto-firmato. Se un dominio viene utilizzato per siti web o applicazioni di clienti esterni ma ha un certificato auto-firmato, i principali browser web visualizzeranno un avviso di sicurezza ai visitatori e impediranno loro di raggiungere il sito. Tutte le applicazioni che utilizzano questo dominio potrebbero non funzionare. Questo non è solo un rischio significativo per la sicurezza, ma potenzialmente dannoso per la fiducia dei vostri clienti nel vostro sito web. Generalmente, i certificati di sicurezza dovrebbero essere rilasciati da un'Autorità di Certificazione di fiducia, ma è possibile utilizzare un certificato auto-firmato solamente per i vostri siti web o le vostre applicazioni interne. Vi raccomandiamo di aggiornare il certificato di sicurezza ad uno di un'Autorità di Certificazione di fiducia per essere al sicuro.

High Risk: 16
Data: 07/11/2020
Categoria:
Certificato
Argomento:
Certificato di sicurezza

mail.plastitomax.com ha un certificato auto-firmato. Se un dominio viene utilizzato per siti web o applicazioni di clienti esterni ma ha un certificato auto-firmato, i principali browser web visualizzeranno un avviso di sicurezza ai visitatori e impediranno loro di raggiungere il sito. Tutte le applicazioni che utilizzano questo dominio potrebbero non funzionare. Questo non è solo un rischio significativo per la sicurezza, ma potenzialmente dannoso per la fiducia dei vostri clienti nel vostro sito web. Generalmente, i certificati di sicurezza dovrebbero essere rilasciati da un'Autorità di Certificazione di fiducia, ma è possibile utilizzare un certificato auto-firmato solamente per i vostri siti web o le vostre applicazioni interne. Vi raccomandiamo di aggiornare il certificato di sicurezza ad uno di un'Autorità di Certificazione di fiducia per essere al sicuro.

High Risk: 17
Data: 07/11/2020
Categoria:
Certificato
Argomento:
Certificato di sicurezza

webmail.plastitomax.com ha un certificato auto-firmato. Se un dominio viene utilizzato per siti web o applicazioni di clienti esterni ma ha un certificato auto-firmato, i principali browser web visualizzeranno un avviso di sicurezza ai visitatori e impediranno loro di raggiungere il sito. Tutte le applicazioni che utilizzano questo dominio potrebbero non funzionare. Questo non è solo un rischio significativo per la sicurezza, ma potenzialmente dannoso per la fiducia dei vostri clienti nel vostro sito web. Generalmente, i certificati di sicurezza dovrebbero essere rilasciati da un'Autorità di Certificazione di fiducia, ma è possibile utilizzare un certificato auto-firmato solamente per i vostri siti web o le vostre applicazioni interne. Vi raccomandiamo di aggiornare il certificato di sicurezza ad uno di un'Autorità di Certificazione di fiducia per essere al sicuro.

!	**High Risk:** 18 **Data:** 07/11/2020 **Categoria:** Certificato **Argomento:** Certificato di sicurezza	**www.plastitomax.com** ha un certificato auto-firmato. Se un dominio viene utilizzato per siti web o applicazioni di clienti esterni ma ha un certificato auto-firmato, i principali browser web visualizzeranno un avviso di sicurezza ai visitatori e impediranno loro di raggiungere il sito. Tutte le applicazioni che utilizzano questo dominio potrebbero non funzionare. Questo non è solo un rischio significativo per la sicurezza, ma potenzialmente dannoso per la fiducia dei vostri clienti nel vostro sito web. Generalmente, i certificati di sicurezza dovrebbero essere rilasciati da un'Autorità di Certificazione di fiducia, ma è possibile utilizzare un certificato auto-firmato solamente per i vostri siti web o le vostre applicazioni interne. Vi raccomandiamo di aggiornare il certificato di sicurezza ad uno di un'Autorità di Certificazione di fiducia per essere al sicuro.
!	**High Risk:** 19 **Data:** 07/11/2020 **Categoria:** E-mail **Argomento:** Policy di email spoofing	**@webplastitomax.com** non dispone di una policy DMARC per impedire che le email contraffatte vengano consegnate alle caselle di posta in arrivo dei destinatari. Anche se si dispone di soluzioni di protezione della posta in entrata, queste non impediranno ai criminali di inviare email contraffatte ai vostri clienti, fornitori e altri contatti commerciali vitali!
!	**High Risk:** 20 **Data:** 07/11/2020 **Categoria:** E-mail **Argomento:** Policy di email spoofing	**@plastitomax.com** non dispone di una policy DMARC per impedire che le email contraffatte vengano consegnate alle caselle di posta in arrivo dei destinatari. Anche se si dispone di soluzioni di protezione della posta in entrata, queste non impediranno ai criminali di inviare email contraffatte ai vostri clienti, fornitori e altri contatti commerciali vitali!
!	**High Risk:** 21 **Data:** 07/11/2020 **Categoria:** E-mail **Argomento:** Protezione mittente email	**@webplastitomax.com** non specifica i mittenti autorizzati. Questo significa che chiunque può inviare una email fingendo di essere da **@webplastitomax.com**, e i destinatari non possono confermare che le email provengano realmente da voi! È necessario impostare un record SPF (Sender Protection Framework) del DNS per **webplastitomax.com** per specificare quali server possono inviare email per vostro conto, ed escludere altri dall'invio di email che fingono di essere voi. Anche se si dispone di soluzioni di protezione della posta in entrata, queste non impediranno ai criminali di inviare email contraffatte ai vostri clienti, fornitori e altri contatti commerciali vitali!

Medium Risk

Colore	Dettagli	Descrizione
!	**Medium Risk:** 1 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	La versione di **Postfix smtpd** utilizzata sulla porta **587** e l'indirizzo IP **93.51.142.18** non è rilevabile. Perché è così importante? Le versioni più aggiornate dei prodotti garantisco che eventuali bug o vulnerabilità siano corretti al fine di mantenere la massima sicurezza. Più vecchia è la versione, più è probabile che abbia delle vulnerabilità. Le versioni più vecchie dei servizi sono meno supportate dagli sviluppatori, rendendo un'organizzazione più vulnerabile agli attacchi informatici e al fallimento del servizio. Si dovrebbe verificare che il prodotto in esecuzione sia aggiornato alla versione più aggiornata.
!	**Medium Risk:** 2 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	La versione di **Postfix smtpd** utilizzata sulla porta **25** e l'indirizzo IP **93.51.142.18** non è rilevabile. Perché è così importante? Le versioni più aggiornate dei prodotti garantisco che eventuali bug o vulnerabilità siano corretti al fine di mantenere la massima sicurezza. Più vecchia è la versione, più è probabile che abbia delle vulnerabilità. Le versioni più vecchie dei servizi sono meno supportate dagli sviluppatori, rendendo un'organizzazione più vulnerabile agli attacchi informatici e al fallimento del servizio. Si dovrebbe verificare che il prodotto in esecuzione sia aggiornato alla versione più aggiornata.
!	**Medium Risk:** 3 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	La versione di **Postfix smtpd** utilizzata sulla porta **465** e l'indirizzo IP **93.51.142.18** non è rilevabile. Perché è così importante? Le versioni più aggiornate dei prodotti garantisco che eventuali bug o vulnerabilità siano corretti al fine di mantenere la massima sicurezza. Più vecchia è la versione, più è probabile che abbia delle vulnerabilità. Le versioni più vecchie dei servizi sono meno supportate dagli sviluppatori, rendendo un'organizzazione più vulnerabile agli attacchi informatici e al fallimento del servizio. Si dovrebbe verificare che il prodotto in esecuzione sia aggiornato alla versione più aggiornata.
!	**Medium Risk:** 4 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	La versione di **Pure-FTPd** utilizzata sulla porta **21** e l'indirizzo IP **185.6.72.90** non è rilevabile. Perché è così importante? Le versioni più aggiornate dei prodotti garantisco che eventuali bug o vulnerabilità siano corretti al fine di mantenere la massima sicurezza. Più vecchia è la versione, più è probabile che abbia delle vulnerabilità. Le versioni più vecchie dei servizi sono meno supportate dagli sviluppatori, rendendo un'organizzazione più vulnerabile agli attacchi informatici e al fallimento del servizio. Si dovrebbe verificare che il prodotto in esecuzione sia aggiornato alla versione più aggiornata.
!	**Medium Risk:** 5 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Software non aggiornato	La versione del prodotto **Microsoft IIS httpd 10.0** non è l'ultima resa disponibile dal fornitore. Questo servizio utilizza la porta **443** sull'indirizzo IP **93.51.142.28**. Sono disponibili versioni più recenti del prodotto per garantire che eventuali bug o vulnerabilità siano corretti al fine di mantenere la massima sicurezza. Più vecchia è la versione, più è probabile che abbia delle vulnerabilità. Le versioni più vecchie dei servizi sono meno supportate dagli sviluppatori, rendendo un'organizzazione più vulnerabile agli attacchi informatici e al fallimento del servizio. Cosa dovreste fare? Per mantenere una sicurezza ottimale e prevenire gli attacchi informatici, potrebbe essere preferibile una versione più recente di questo prodotto.
!	**Medium Risk:** 6 **Data:** 07/11/2020 **Categoria:** Servizio **Argomento:** Pericolo potenziale	**FTP server file_server** sta attualmente utilizzando la porta **21** sull'indirizzo IP **93.51.142.25**. C'è la possibilità che questa porta sia direttamente visibile e accessibile da Internet. Una 'porta' è un punto di arrivo di comunicazione per il software in esecuzione su una rete del computer. Gli hacker, quando attaccano un'organizzazione, eseguono una 'scansione porte' sulla rete di destinazione, alla ricerca di porte 'aperte' per identificare i servizi con vulnerabilità che poi sfruttano. Avere una porta aperta rende un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Vi raccomandiamo di controllare, in quanto c'è un rischio reale di essere vulnerabile agli attacchi esterni, nel qual caso è necessario proteggersi con un firewall o chiudere l'accesso alla porta.

Medium Risk: 7
Data: 07/11/2020
Categoria: Servizio
Argomento: Pericolo potenziale

FTP server file_server sta attualmente utilizzando la porta **21** sull'indirizzo IP **178.236.175.252**. C'è la possibilità che questa porta sia direttamente visibile e accessibile da Internet. Una 'porta' è un punto di arrivo di comunicazione per il software in esecuzione su una rete del computer. Gli hacker, quando attaccano un'organizzazione, eseguono una 'scansione porte' sulla rete di destinazione, alla ricerca di porte 'aperte' per identificare i servizi con vulnerabilità che poi sfruttano. Avere una porta aperta rende un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Vi raccomandiamo di controllare, in quanto c'è un rischio reale di essere vulnerabile agli attacchi esterni, nel qual caso è necessario proteggersi con un firewall o chiudere l'accesso alla porta.

Medium Risk: 8
Data: 07/11/2020
Categoria: Servizio
Argomento: Pericolo potenziale

SSH or SFTP developer_access sta attualmente utilizzando la porta **2222** sull'indirizzo IP **91.212.167.73**. C'è la possibilità che questa porta sia direttamente visibile e accessibile da Internet. Una 'porta' è un punto di arrivo di comunicazione per il software in esecuzione su una rete del computer. Gli hacker, quando attaccano un'organizzazione, eseguono una 'scansione porte' sulla rete di destinazione, alla ricerca di porte 'aperte' per identificare i servizi con vulnerabilità che poi sfruttano. Avere una porta aperta rende un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Vi raccomandiamo di controllare, in quanto c'è un rischio reale di essere vulnerabile agli attacchi esterni, nel qual caso è necessario proteggersi con un firewall o chiudere l'accesso alla porta.

Medium Risk: 9
Data: 07/11/2020
Categoria: Servizio
Argomento: Pericolo potenziale

Clock Synchronisation clock_synchronisation sta attualmente utilizzando la porta **123** sull'indirizzo IP **93.51.142.25**. C'è la possibilità che questa porta sia direttamente visibile e accessibile da Internet. Una 'porta' è un punto di arrivo di comunicazione per il software in esecuzione su una rete del computer. Gli hacker, quando attaccano un'organizzazione, eseguono una 'scansione porte' sulla rete di destinazione, alla ricerca di porte 'aperte' per identificare i servizi con vulnerabilità che poi sfruttano. Avere una porta aperta rende un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Vi raccomandiamo di controllare, in quanto c'è un rischio reale di essere vulnerabile agli attacchi esterni, nel qual caso è necessario proteggersi con un firewall o chiudere l'accesso alla porta.

Medium Risk: 10
Data: 07/11/2020
Categoria: Servizio
Argomento: Pericolo potenziale

Clock Synchronisation clock_synchronisation sta attualmente utilizzando la porta **123** sull'indirizzo IP **93.51.142.28**. C'è la possibilità che questa porta sia direttamente visibile e accessibile da Internet. Una 'porta' è un punto di arrivo di comunicazione per il software in esecuzione su una rete del computer. Gli hacker, quando attaccano un'organizzazione, eseguono una 'scansione porte' sulla rete di destinazione, alla ricerca di porte 'aperte' per identificare i servizi con vulnerabilità che poi sfruttano. Avere una porta aperta rende un'organizzazione estremamente vulnerabile agli attacchi informatici e al fallimento del servizio. Vi raccomandiamo di controllare, in quanto c'è un rischio reale di essere vulnerabile agli attacchi esterni, nel qual caso è necessario proteggersi con un firewall o chiudere l'accesso alla porta.

Medium Risk: 11
Data: 07/11/2020
Categoria: Certificato
Argomento:

Il certificato di **plastitomax.com** non include **plastitomax.com** nei nomi validi. I certificati sono validi solo per i sottodomini che sono inclusi nella loro lista di domini validi. Le connessioni di visitatori a **plastitomax.com** non saranno sicure, anche se dopo saranno indirizzate al sito sicuro. Questo permette agli hacker di intercettare e modificare quello che vedono in inviano al sito. Se un visitatore naviga su https //**plastitomax.com**, il suo browser mostrerà un alert di sicurezza per prevenire che il sito venga raggiunto. Questo pone a rischio sia la sicurezza del sicurezza e la fiducia del cliente. Dovrebbe essere generato e installato un certificato valido per **plastitomax.com**.

Medium Risk: 12
Data: 07/11/2020
Categoria: Certificato
Argomento:

Il certificato di **mail.plastitomax.com** non include **mail.plastitomax.com** nei nomi validi. I certificati sono validi solo per i sottodomini che sono inclusi nella loro lista di domini validi. Le connessioni di visitatori a **mail.plastitomax.com** non saranno sicure, anche se dopo saranno indirizzate al sito sicuro. Questo permette agli hacker di intercettare e modificare quello che vedono in inviano al sito. Se un visitatore naviga su https //**mail.plastitomax.com**, il suo browser mostrerà un alert di sicurezza per prevenire che il sito venga raggiunto. Questo pone a rischio sia la sicurezza del sicurezza e la fiducia del cliente. Dovrebbe essere generato e installato un certificato valido per **mail.plastitomax.com**.

Medium Risk: 13
Data: 07/11/2020
Categoria: Certificato
Argomento: Certificato di sicurezza

Il certificato che si sta attualmente utilizzando per **push.plastitomax.com** sta per scadere il **2020-12-01**. Se un dominio supporta servizi accessibili dall'esterno ma il suo certificato è scaduto, i principali browser web visualizzeranno un avviso di sicurezza ai visitatori e impediranno loro di raggiungere il sito. Tutte le applicazioni che utilizzano questo dominio non funzioneranno più. Questo non è solo un rischio significativo per la sicurezza, ma potenzialmente dannoso per la fiducia dei vostri clienti nel vostro sito web. Vi suggeriamo di contattare un'Autorità di Certificazione di fiducia per sostituire questo certificato prima della **2020-12-01** per mantenere la sicurezza e l'operatività ininterrotta dei servizi su questo dominio.

Medium Risk: 14
Data: 07/11/2020
Categoria: Certificato
Argomento:

Il certificato di **webmail.webplastitomax.com** non include **webmail.webplastitomax.com** nei nomi validi. I certificati sono validi solo per i sottodomini che sono inclusi nella loro lista di domini validi. Le connessioni di visitatori a **webmail.webplastitomax.com** non saranno sicure, anche se dopo saranno indirizzate al sito sicuro. Questo permette agli hacker di intercettare e modificare quello che vedono in inviano al sito. Se un visitatore naviga su https //**webmail.webplastitomax.com**, il suo browser mostrerà un alert di sicurezza per prevenire che il sito venga raggiunto. Questo pone a rischio sia la sicurezza del sicurezza e la fiducia del cliente. Dovrebbe essere generato e installato un certificato valido per **webmail.webplastitomax.com**.

Medium Risk: 15
Data: 07/11/2020
Categoria: Certificato
Argomento:

Il certificato di **webmail.plastitomax.com** non include **webmail.plastitomax.com** nei nomi validi. I certificati sono validi solo per i sottodomini che sono inclusi nella loro lista di domini validi. Le connessioni di visitatori a **webmail.plastitomax.com** non saranno sicure, anche se dopo saranno indirizzate al sito sicuro. Questo permette agli hacker di intercettare e modificare quello che vedono in inviano al sito. Se un visitatore naviga su https //**webmail.plastitomax.com**, il suo browser mostrerà un alert di sicurezza per prevenire che il sito venga raggiunto. Questo pone a rischio sia la sicurezza del sicurezza e la fiducia del cliente. Dovrebbe essere generato e installato un certificato valido per **webmail.plastitomax.com**.

Medium Risk: 16
Data: 07/11/2020
Categoria: Certificato
Argomento:

Il certificato di **www.plastitomax.com** non include **www.plastitomax.com** nei nomi validi. I certificati sono validi solo per i sottodomini che sono inclusi nella loro lista di domini validi. Le connessioni di visitatori a **www.plastitomax.com** non saranno sicure, anche se dopo saranno indirizzate al sito sicuro. Questo permette agli hacker di intercettare e modificare quello che vedono in inviano al sito. Se un visitatore naviga su https //**www.plastitomax.com**, il suo browser mostrerà un alert di sicurezza per prevenire che il sito venga raggiunto. Questo pone a rischio sia la sicurezza del sicurezza e la fiducia del cliente. Dovrebbe essere generato e installato un certificato valido per **www.plastitomax.com**.

Dominio

Dominio	Dettagli di registrazione	Rischi	Sottodomini
plastitomax.com	Email registrata: raffallo.sanzio@plastitomax.com Registrato: TUCOWS DOMAINS INC.	1 High Risk 0 Medium Risk 3 Low Risk	24
webplastitomax.com	Email registrata: leonardo.davinci@plastitomax.com Registrato: TUCOWS DOMAINS INC.	1 High Risk 0 Medium Risk 3 Low Risk	7