RILEVA E PREVIENI LA PERDITA DI DATI

I 5 PUNTI DELLA CYBERSECURITY

RBR verona

IL TUO PARTNER TECNOLOGICO PER ICT E SICUREZZA

1.Identificazione delle minacce: è fondamentale identificare le minacce informatiche per poterle prevenire e contrastare. La conoscenza delle minacce più comuni e delle tecniche utilizzate dai cyber criminali è essenziale per la sicurezza dei sistemi.

2. Protezione dei dati: la protezione dei dati sensibili è fondamentale per evitare violazioni e perdite di dati. È importante utilizzare tecniche e strumenti per la crittografia dei dati, per la gestione delle password e per la protezione degli endpoint.

3. Operativa: la possibilità di interruzione delle attività aziendali a causa di attacchi informatici può causare perdite finanziarie e danni alla reputazione. È importante avere piani di continuità operativa per garantire la resilienza dell'azienda in caso di attacchi.

4.Conformità normativa: le aziende devono aderire a numerose norme e regolamentazioni per la sicurezza dei dati, come il GDPR. È importante garantire la conformità a queste norme per evitare sanzioni e sanzioni.

5.Sicurezza degli utenti: la sicurezza degli utenti è un aspetto fondamentale della cybersecurity. È importante sensibilizzare gli utenti sui rischi e su come evitare di diventare vittime di attacchi informatici, attraverso la formazione e la diffusione di buone pratiche di sicurezza.

Checklist di sicurezza informatica aziendale:

1. Identificazione delle minacce: effettuare un'analisi delle minacce per identificare le minacce più comuni e le tecniche utilizzate dai cyber criminali.
2. Protezione dei dati: configurare le politiche di sicurezza per proteggere i dati sensibili dell'azienda.
3. Continuità operativa: creare piani di continuità operativa per garantire la resilienza dell'azienda in caso di attacchi informatici.
4. Conformità normativa: verificare la conformità alle normative e alle regolamentazioni per evitare sanzioni e sanzioni.
5. Sicurezza degli utenti: sensibilizzare gli utenti sui rischi e su come evitare di diventare vittime di attacchi informatici attraverso la formazione e la diffusione di buone pratiche di sicurezza.
6. Sistemi di sicurezza: installare e configurare i sistemi di sicurezza (firewall, antivirus, antimalware, intrusion prevention system) per proteggere la rete aziendale.
7. Sicurezza delle reti: monitorare e proteggere le reti aziendali per prevenire attacchi interni e malware.
8. Sicurezza degli endpoint: proteggere i sistemi dell'azienda da attacchi esterni e interni.
9. Sicurezza delle email: proteggere le email aziendali da phishing e malware.
10. Monitoraggio

I RISCHI PER LA TUA AZIENDA

La cybersecurity è una preoccupazione crescente per le aziende di tutto il mondo, poiché le minacce informatiche diventano sempre più sofisticate e diffuse.

I rischi per la sicurezza informatica includono attacchi esterni e interni, perdita di dati, conformità normativa e interruzione delle attività aziendali.

Le aziende devono implementare soluzioni di sicurezza informatica efficaci e sensibilizzare i dipendenti sui rischi, proteggendo la propria azienda da possibili data breach e perdita dei dati aziendali.

Protezione dei dati sensibili

La perdita o la violazione dei dati sensibili può causare danni finanziari e legali significativi per un'azienda. Investire in cybersecurity permette di proteggere i propri dati e prevenire violazioni.

Conformità normativa

Le aziende devono aderire a numerose norme e regolamentazioni per la sicurezza dei dati, come il GDPR. Investire in cybersecurity permette di garantire la conformità a queste norme e di evitare sanzioni dal Garante.

Continuità operativa

Gli attacchi informatici possono interrompere le attività aziendali, causando perdite finanziarie e compromettendo la continuità operativa. Investire in cybersecurity permette di proteggere la propria azienda da questi attacchi e di garantire la continuità operativa.

Reputazione aziendale

La reputazione aziendale è un fattore chiave per il successo dell'azienda. Investire in cybersecurity permette di proteggere la reputazione aziendale evitando violazioni dei dati e garantendo la sicurezza dei propri clienti.

Protezione degli asset aziendali

Gli attacchi informatici possono compromettere i sistemi aziendali e i dati, causando perdite finanziarie e danni alla reputazione. Investire in cybersecurity permette di proteggere gli asset aziendali e di garantire la sicurezza dell'azienda.

Il tuo sistema informatico è al sicuro?

Siamo consapevoli che in un mondo sempre più connesso, la sicurezza delle informazioni è diventata una preoccupazione sempre più importante per tutti noi.

Ogni giorno, infatti, sono sempre più frequenti gli attacchi informatici che mettono a rischio la sicurezza dei nostri dati personali e delle nostre attività online.

È per questo che forniamo un prodotto unico nel suo genere: un servizio di controllo che ti permette di proteggere il tuo business dalle minacce informatiche.

Con il nostro servizio, potrai dormire sonni tranquilli sapendo che i tuoi dati e le tue attività online sono al sicuro.

Grazie alla nostra tecnologia all'avanguardia siamo in grado di rilevare e bloccare qualsiasi tentativo di attacco informatico, garantendo così la massima sicurezza delle informazioni.

Inoltre, il nostro team di esperti è sempre pronto ad assisterti in caso di necessità.

Non correre rischi inutili: proteggi il tuo business con il nostro servizio di controllo.

RBR Group **protegge dati**, **sistemi di rete** e **connessioni internet** delle aziende, con tecnologie all’avanguardia per la sicurezza IT.

Spiccano tra le nostre proposte **firewall** e **router** di ultima generazione, studiati per assicurare sia un elevato livello di protezione da minacce, esterne e interne, che una piena razionalizzazione delle infrastrutture di rete.

Negli anni abbiamo acquisito numerose certificazioni per qualificarci come esperti di settore.

CASE STUDY RBR

Il cliente in questione è un'azienda di medie dimensioni situata a Verona e specializzata nella produzione di componenti meccanici.

Dopo aver installato la sonda del Cyber Command, da noi fortemente consigliata, ha scoperto che il suo sistema informatico presentava numerose falle di sicurezza.

In particolare, è stato rilevato che il firewall dell'azienda non era adeguatamente configurato e che esistevano vulnerabilità nei sistemi operativi e nei software in uso.

Inoltre, è stato individuato un tentativo di hacking che era stato bloccato solo in parte dal sistema di sicurezza in uso e che protratto nel tempo avrebbe portato al blocco di tutta l'infrastruttura informatica aziendale.

Dopo aver identificato queste problematiche, il team di RBR Verona ha lavorato con il cliente per implementare una serie di misure volte a correggere le falle di sicurezza e a rafforzare la protezione del sistema informatico dell'azienda.

Sono state adottate soluzioni di sicurezza avanzate, come il rafforzamento delle password e la creazione di un sistema di autenticazione a due fattori, e sono stati eseguiti test di penetrazione per verificare la robustezza del sistema.

Il risultato finale è stato un sistema informatico più sicuro e protetto, che ha permesso al cliente di aumentare la produttività e di ridurre il rischio di attacchi informatici.

Con la nostra piattaforma di gestione della sicurezza informatica, gli amministratori di sistema possono monitorare e gestire in modo centralizzato la sicurezza della rete aziendale, rilevando e risolvendo rapidamente eventuali minacce.

CYBER COMMAND

SANGFOR

Un'interfaccia utente unificata per la **gestione e il monitoraggio della sicurezza della tua rete.**

Il sistema Sangfor consente agli amministratori di sicurezza di avere una visione d'insieme delle minacce e poter prendere decisioni informate in tempo reale.

Richiedi
un test gratuito

TEST

10 controlli di CyberCommand per garantire la sicurezza della tua azienda:

1. **Controllo delle minacce esterne**: rilevamento e prevenzione di attacchi informatici come malware, phishing e attacchi DDoS.
2. **Controllo dell'accesso**: monitoraggio e controllo dell'accesso ai dati sensibili dell'azienda per prevenire l'accesso non autorizzato.
3. **Controllo della perdita di dati**: rilevamento e prevenzione della perdita di dati per proteggere i dati dell'azienda da possibili violazioni.
4. **Controllo della conformità normativa**: verifica della conformità alle normative e alle regolamentazioni per evitare sanzioni e sanzioni.
5. **Controllo della sicurezza delle applicazioni**: verifica della sicurezza delle applicazioni utilizzate dall'azienda per prevenire vulnerabilità e attacchi.
6. **Controllo della sicurezza delle password**: verifica della sicurezza delle password per prevenire l'accesso non autorizzato.
7. **Controllo della sicurezza delle reti**: verifica della sicurezza delle reti per proteggere la rete aziendale da attacchi interni e malware.
8. **Controllo della sicurezza degli endpoint**: verifica della sicurezza degli endpoint per proteggere i sistemi dell'azienda da attacchi esterni e interni.
9. **Controllo della sicurezza delle email**: verifica della sicurezza delle email per prevenire la diffusione di malware e phishing.
10. **Controllo della sicurezza degli utenti**: verifica della sicurezza degli utenti per prevenire l'accesso non autorizzato e garantire la conformità alle politiche aziendali.


1
Rileva le minacce sconosciute che rappresentano un rischio potenziale per l'organizzazione
2
Migliore visibilità della strategia di sicurezza dell'infrastruttura
3
L'analisi dell'impatto aziendale rileva eventuali aree compromesse e aiuta a definire le priorità di mitigazione
4
Una risposta più rapida migliora il controllo generale della sicurezza
5
Più conveniente di altre soluzioni (es. SIEM)

Come partecipare gratuitamente al test di valutazione della tua rete?

Giorno 1

- Installazione dei dispositivi e configurazione del traffico di mirror
- Adeguamento della configurazione in base alla topologia della tua rete aziendale

Giorno 7

- Sessione remota per verificare i risultati del rilevamento
- Creazione di un report intermedio per presentare i risultati
- Creazione di automatismi di risposta automatica per la correzione (opzionale)
- Dimostrare le capacità di integrazione con le altre tecnologie (opzionale)

Giorno 9

- Controllo dei risultati in loco
- Controllo della cronologia delle operazioni di correzione
- Cancellazione dei dati personali e recupero dei dispositivi di prova
- Pianificazione della revisione dei risultati della POC (ultimo giorno)

Ultimo giorno

- Riassunto e presentazione dei risultati del test
- Consigli su come migliorare la rete
- Q&A

CERTIFICAZIONI

CYSA+ (CompTIA Cybersecurity Analyst) è un certificazione professionale rilasciata dalla CompTIA (Computing Technology Industry Association) che dimostra le competenze nell'analisi delle minacce informatiche e nella gestione della sicurezza delle informazioni.

La certificazione è progettata per gli individui che svolgono funzioni di analista di sicurezza informatica, come la gestione delle minacce, la protezione dei dati e la conformità normativa.

Il processo di certificazione CYSA+ include un esame scritto che verifica le competenze in materia di:

- Analisi delle minacce
- Protezione dei dati
- Compliance e vulnerabilità
- Gestione delle minacce
- Sicurezza delle reti

La certificazione CYSA+ è riconosciuta a livello globale e dimostra che l'individuo ha le competenze necessarie per proteggere le reti e i sistemi dell'azienda dalle minacce informatiche.

CYBER COMMAND

REQUISITI MINIMI DI CONFIGURAZIONE

IL DEPLOYMENT È COMPATIBILE SOLO CON VMWARE ESXI 6.0 E VMWARE ESXI 7.0.

IL PROCESSORE COMPATIBILE AVX DEVE ESSERE SUPPORTATO DALL'HOST DELLA CLOUD STA.

LA MACCHINA VIRTUALE DOVREBBE ESSERE CONFIGURATA CON ALMENO TRE NIC VIRTUALI, E LA NIC SUPPORTA SOLO VMXNET3.

REQUISITI MINIMI:

- *2 SCHEDE RETE FISICHE*
- *16VCORE*
- *16 GB RAM*
- *1 HDD 128GB*
- *2 HDD 128GB/256GB*

RBR verona

RBR verona

Il partner unico per ICT e Sicurezza

CONTATTI

Via Monsignor Gentilin, 62,
37132 Verona (VR)

045 840 3665

https://www.rbrverona.it/