baramundi

Le **CHECK-LIST BARAMUNDI** forniscono consigli concisi, passo dopo passo, per gestire in modo semplice le sfide informatiche più comuni. Altre check-list sono disponibili su **www.baramundi.com/check-list**

Attacchi di phishing – 5 strategie di prevenzione

La parola "phishing" utilizza le prime lettere delle parole "password harvesting" al posto della "f" di "fishing". Si tratta di messaggi di testo, vocali o di posta elettronica inviati da hacker camuffati da contatti noti o istituzioni che chiedono alle vittime informazioni sensibili sui conti o trasferimenti elettronici di denaro. Le richieste fasulle chiedono alle vittime informazioni importanti (ad esempio, dati di login, numeri di conto, ecc.) o addirittura impongono loro di effettuare bonifici bancari. Ma come si riconosce il phishing?

Indirizzo del mittente

Controllare se l'indirizzo o il numero del mittente corrispondono a un contatto noto e verificato. Gli errori ortografici, grammaticali e di altro tipo sono segnali di allarme.

Nome del dominio

Controllare sempre ciò che viene dopo la @ nell'indirizzo e-mail del mittente. Gli indirizzi con errori di battitura o con un'ortografia modificata che assomiglia a un indirizzo legittimo sono inganni comuni.

Spoofing

I criminali spesso inviano messaggi che utilizzano il nome e l'indirizzo di un contatto legittimo, persino il vostro! Ecco perché non ci si può basare solo su nomi o indirizzi che sembrano corretti. Un'attenta lettura del contenuto del messaggio può essere d'aiuto. Misure tecniche come il controllo del Reply-to, del server, dell'autenticazione, dell'instradamento e di altri dati presenti nell'header di un'e-mail possono aiutare a determinare se un messaggio è falso o legittimo.

Link e allegati pericolosi

Il phishing spesso induce le vittime a scaricare malware tramite link o documenti allegati. Prima di fare clic su un messaggio, visualizzate sempre l'URL incorporato nel testo o nella grafica, posizionando il cursore su di esso per alcuni secondi. Non cliccate su un allegato a meno che non l'abbiate richiesto o atteso e siate sicuri al 100% che sia sicuro.

Verifica

Il phishing sfrutta la fiducia e la paura delle vittime. È molto più sicuro verificare qualsiasi messaggio di testo, vocale o di posta elettronica sospetto utilizzando un indirizzo web o un numero di telefono affidabile per contattare il mittente. Le aziende e le agenzie governative sono consapevoli degli attacchi di phishing e vogliono aiutare le persone a evitare le truffe.

In sintesi: Gli attacchi di phishing rimangono un rischio significativo. I dipendenti attenti sono fondamentali per identificare i link pericolosi e dovrebbero ricevere una formazione continua. Inoltre, la baramundi Management Suite consente aggiornamenti regolari e patch di sicurezza per eliminare ulteriori potenziali vulnerabilità.