ESEMPI DI DOMANDE

per un'indagine sulla Sicurezza Informatica Interna

Data Security Guide

Esempi di domande per un'indagine sulla Sicurezza Informatica Interna

Le domande a seguire possono costituire uno strumento utile alla creazione di un questionario sulla sicurezza interna dell'azienda. Completate e adattate alle specificità della propria azienda, potrebbero aiutare a identificare le principali lacune da colmare e le sfide da affrontare.

1. Come comportarsi in caso di una divulgazione della password aziendale? (scelta multipla)

a) Non fare nulla.
b) Cambiare immediatamente la password.
c) Segnalarlo come incidente di sicurezza.
d) Attendere e vedere se succede qualcosa.

2. Qual è la procedura sicura in caso di perdita di un token, di una chiave o di un badge di accesso?

a) Entrare nei locali dell'azienda senza verifica, accompagnato dai propri colleghi o prendere in prestito un token/chiave da un collega.
b) Aspettare un po' di tempo (per esempio, una settimana), e se il token/chiave non è stato ancora trovato, segnalarne la perdita.
c) Segnalare immediatamente lo smarrimento del token/chiave.
d) Richiedere un nuovo token/chiave di accesso per visitatori e usare quello.

3. Come si può proteggere la riservatezza dei dati sensibili inviati per e-mail?

a) Aggiungendo un disclaimer di riservatezza in fondo all'email.
b) In nessun modo; pertanto, non invio dati sensibili via e-mail.
c) Criptando l'e-mail.
d) Firmando l'e-mail.

4. In quali modi un computer può essere infettato da un malware? Selezionare tutte le risposte applicabili.

a) Eseguendo un malware che sembra essere un programma legittimo.
b) Visitando un sito web infetto.
c) Via e-mail - e-mail HTML o allegati (MS Office, PDF).
d) Collegandosi a una rete infetta - in hotel, treno, autobus o hotspot Wi-Fi gratuito.

5. Come si può ridurre al minimo la quantità di spam nella propria casella di posta elettronica aziendale? Selezionare tutte le risposte applicabili.

a) Non usare l'email aziendale per registrarsi a vari servizi non legati al lavoro.
b) Pubblicare il proprio indirizzo e-mail aziendale nei forum pubblici.
c) Registrarsi solo a newsletter affidabili.
d) Usare l'email aziendale esclusivamente per attività legate al lavoro.

6. **Quale delle seguenti opzioni potrebbe aiutare a prevenire che malware e virus infettino il PC?**

a) Scaricare software solo da fonti affidabili.
b) Installare un programma antivirus.
c) Aggiornare sempre il PC quando viene richiesto un aggiornamento del sistema.
d) Tutti i precedenti.

7. **Dove devono essere collocati i dispositivi aziendali (monitor, computer portatili) se vengono utilizzati per elaborare dati classificati come "Confidenziali" o "Strettamente confidenziali"?**

a) Non è importante.
b) Vicino a una finestra.
c) Vicino alle porte.
d) Situato in modo tale che i dati trattati non possano essere visti da personale non autorizzato.

8. **Quali regole/comportamenti devono essere seguiti quando si usano i telefoni cellulari aziendali?** Selezionare tutte le risposte applicabili.

a) Politica di blocco del cellulare e politica delle password.
b) Crittografia del telefono cellulare e della scheda.
c) Installazione di tutte le app a disposizione.
d) Tutti i precedenti.

9. **Stai navigando in un sito web su una rete Wi-Fi pubblica, ma il tuo programma antivirus non è aggiornato. Quale delle seguenti affermazioni è vera?**

a) Il tuo dispositivo collegato alla rete Wi-Fi pubblica è ancora sicuro perché accedi solo a pagine contenenti notizie del tuo paese.
b) La comunicazione via http non può essere intercettata.
c) La comunicazione con i sistemi aziendali tramite VPN è sicura.
d) Nessuna delle affermazioni precedenti è vera.

10. **Quale delle seguenti opzioni aiuta a determinare se un sito di shopping online è affidabile?**

a) L'indirizzo del sito web inizia con "https://".
b) C'è un marchio sul sito web che riporta la dicitura "100% sicuro".
c) Fare delle ricerche per verificare se il sito ha una buona reputazione.
d) Osservare il sito web e cercare le recensioni positive dei clienti.

11. Come vengono messi in atto gli attacchi omografi?

a) Il truffatore sfrutta le somiglianze dei caratteri testuali.
b) Il truffatore invia un allegato infetto.
c) Il truffatore invia la stessa e-mail di phishing a tutti i membri dell'azienda.
d) Nessuna delle precedenti.

12. Quale delle seguenti attività di gestione delle password è sicura?

a) Su richiesta, fornire la password al proprio superiore.
b) Conservare la password su carta in una busta, chiusa a chiave nella propria scrivania.
c) Su richiesta, fornire la password al responsabile della sicurezza interna.
d) Scrivere la password su un pezzo di carta e incollarlo sul retro della tastiera.

13. In che modo gli utenti possono utilizzare le proprie password all'interno di **NOME AZIENDA**?

a) Nessuna restrizione.
b) Le password devono essere complesse. Gli utenti sono autorizzati ad usare le proprie password di **NOME AZIENDA** al di fuori di **NOME AZIENDA**.
c) Le password devono essere complesse. Gli utenti non sono autorizzati ad usare le le proprie password di **NOME AZIENDA** al di fuori di **NOME AZIENDA**.
d) Le password devono essere complesse. Gli utenti sono autorizzati a condividere le password con i propri colleghi.

14. Ricevi una chiamata e l'interlocutore richiede informazioni sensibili. Come si dovrebbe rispondere?

a) Chiedere all'interlocutore di inviare la richiesta tramite un'email firmata da un indirizzo aziendale e verificarne l'identità.
b) Insistere che lo richiamerai al suo telefono.
c) Chiedere il nome del suo responsabile prima di assecondare la richiesta.
d) Soddisfare la richiesta, dato che ora lavorano da casa e non hanno accesso a un telefono aziendale.

15. Qual è il modo migliore per proteggere la riservatezza dei dati memorizzati su un portatile nel caso in cui questo venga rubato?

a) Crittografia completa del disco.
b) Antifurto.
c) Antivirus.
d) Backup.

16. Posso caricare, archiviare ed elaborare dati aziendali riservati in un servizio cloud non autorizzato (Google Docs, Translate, Drive; Dropbox)?

a) Sì.
b) No.

17. Quali informazioni non dovrebbero essere pubblicate su un profilo social privato? Selezionare tutte le risposte applicabili.

a) Informazioni sulle operazioni interne aziendali
b) Email aziendali e altre informazioni di contatto.
c) Storie divertenti su cose fatte in vacanza.
d) Le proprie informazioni personali, come l'indirizzo e il codice fiscale.

18. Perché si deve bloccare lo schermo del proprio dispositivo quando non è in uso?

a) Per evitare che un codice maligno si installi automaticamente.
b) Per evitare che persone non autorizzate possano sfruttare i diritti di accesso per accedere ai dati sul dispositivo.
c) Per eseguire correttamente il backup dei dati dal dispositivo.
d) Per rispettare la legge sul copyright.

19. Scegli quale opzione NON è una buona pratica di sicurezza fisica.

a) In caso di un'interruzione del lavoro, i dipendenti sono obbligati a bloccare i dispositivi ed eseguire nuovamente l'accesso alla ripresa.
b) I dipendenti sono obbligati a rispettare i principi di clear desk (scrivania ordinata) e clear screen (schermo ordinato).
c) I dipendenti hanno l'obbligo di effettuare la manutenzione e le riparazioni dei dispositivi aziendali.
d) I dipendenti non devono visualizzare informazioni sensibili in aree in cui persone non autorizzate possano vederle.

20. Quale livello di conoscenza in termini di sicurezza ti attribuisci?

a) Ottimo.
b) Buono.
c) Debole.
d) Carente.

Risposte corrette

1. Come comportarsi in caso di una divulgazione della password aziendale? (scelta multipla)

a) Non fare nulla.
b) Cambiare immediatamente la password.
c) Segnalarlo come incidente di sicurezza.
d) Attendere e vedere se succede qualcosa.

Risposte corrette: b), c)

Spiegazione: Come riportato nella **Politica sulla Sicurezza delle Informazioni per i Dipendenti (inserire il riferimento alle proprie politiche di sicurezza)**, in caso di divulgazione della password, il dipendente deve immediatamente cambiare la password e segnalare l'incidente di sicurezza.

2. Qual è la procedura sicura in caso di perdita di un token, di una chiave o di un badge di accesso?

a) Entrare nei locali dell'azienda senza verifica, accompagnato dai propri colleghi o prendere in prestito un token/chiave da un collega.
b) Aspettare un po' di tempo (per esempio, una settimana), e se il token/chiave non è stato ancora trovato, segnalarne la perdita.
c) Segnalare immediatamente lo smarrimento del token/chiave.
d) Richiedere un nuovo token/chiave di accesso per visitatori e usare quello.

Risposta corretta: c)

Spiegazione: È necessario segnalare immediatamente lo smarrimento di un token/chiave in modo che possa essere disattivato per prevenire possibili abusi e ingressi non autorizzati.

3. Come si può proteggere la riservatezza dei dati sensibili inviati per e-mail?

a) Aggiungendo un disclaimer di riservatezza in fondo all'email.
b) In nessun modo; pertanto, non invio dati sensibili via e-mail.
c) Criptando l'e-mail.
d) Firmando l'e-mail.

Risposta corretta: c)

Spiegazione: I messaggi di posta elettronica possono essere intercettati da un aggressore sia quando sono memorizzati su un server di posta elettronica sia quando viaggiano su Internet. La firma digitale dimostra al destinatario che è stato firmato il messaggio e che il contenuto non è stato alterato durante il transito, ma non rende i messaggi illeggibili. La crittografia rende i messaggi illeggibili dal punto in cui iniziano il loro viaggio fino al punto in cui il destinatario li apre. Si possono usare funzioni di crittografia basate su certificati digitali integrati nel proprio servizio di posta elettronica, o scaricare un altro software di crittografia (per esempio, PGP/GPG).

4. In quali modi un computer può essere infettato da un malware? Selezionare tutte le risposte applicabili.

a) Eseguendo un malware che sembra essere un programma legittimo.
b) Visitando un sito web infetto.
c) Via e-mail - e-mail HTML o allegati (MS Office, PDF).
d) Collegandosi a una rete infetta - in hotel, treno, autobus o hotspot Wi-Fi gratuito.

Risposte corrette: a), b), c), d)

Spiegazione: Eseguire un malware che sembra essere un programma legittimo o un'applicazione mobile, visitare siti web infetti, usare la posta elettronica e connettersi a una rete infetta sono tutte modalità comuni per infettare un computer.

5. Come si può ridurre al minimo la quantità di spam nella propria casella di posta elettronica aziendale? Selezionare tutte le risposte applicabili.

a) Non usare l'email aziendale per registrarsi a vari servizi non legati al lavoro.
b) Pubblicare il proprio indirizzo e-mail aziendale nei forum pubblici.
c) Registrarsi solo a newsletter affidabili.
d) Usare l'email aziendale esclusivamente per attività legate al lavoro.

Risposte corrette: a), c), d)

Spiegazione: Per ridurre al minimo la quantità di spam nella casella di posta elettronica aziendale, si dovrebbe essere cauti nel pubblicare il proprio indirizzo e-mail aziendale su siti web pubblici, nelle chat room, in forum pubblici, social network e così via. Si dovrebbe usare un indirizzo email diverso da quello aziendale quando si usa la posta elettronica per le attività private. Rispondere ai messaggi e-mail solo se ritenuti affidabili. Se il messaggio desta sospetti e non ci si fida del mittente, verificarne la legittimità prima di rispondere. Questo vale anche per la cancellazione dalle liste di distribuzione di posta elettronica. Rispondere allo spam conferma allo spammer che il proprio indirizzo email è valido e attivo.

6. Quale delle seguenti opzioni potrebbe aiutare a prevenire che malware e virus infettino il PC?

a) Scaricare software solo da fonti affidabili.
b) Installare un programma antivirus.
c) Aggiornare sempre il PC quando viene richiesto un aggiornamento del sistema.
d) Tutti i precedenti.

Risposta corretta: d)

Spiegazione: Tutte le opzioni possono essere utilizzate per evitare che malware e virus infettino il PC.

7. Dove devono essere collocati i dispositivi aziendali (monitor, computer portatili) se vengono utilizzati per elaborare dati classificati come "Confidenziali" o "Strettamente confidenziali"?

a) Non è importante.
b) Vicino a una finestra.
c) Vicino alle porte.
d) Situato in modo tale che i dati trattati non possano essere visti da personale non autorizzato.

Risposta corretta: d)

Spiegazione: I dispositivi che elaborano dati classificati come "confidenziali" o "strettamente confidenziali" devono essere collocati in modo da ridurre al minimo il rischio che i dati così elaborati possano essere visti da personale non autorizzato.

8. Quali regole/comportamenti devono essere seguiti quando si usano i telefoni cellulari aziendali?

Selezionare tutte le risposte applicabili.

a) Politica di blocco del cellulare e politica delle password.
b) Crittografia del telefono cellulare e della scheda.
c) Installazione di tutte le app a disposizione.
d) Tutti i precedenti.

Risposte corrette: a), b)

Spiegazione: Le buone pratiche e le politiche di gestione dei dispositivi mobili (MDM, mobile device management) raccomandano di proteggere i dati sui telefoni cellulari da accessi fisici e logici non autorizzati utilizzando i seguenti strumenti:

1. Politica di blocco del cellulare e politica delle password.

2. Crittografia del telefono cellulare (e della scheda, se il telefono cellulare ne è dotato) e divieto di utilizzo di applicazioni al di fuori di fonti affidabili (iTunes, Google Play e MDM market). Quando s installa un'applicazione, scegliere quelle che sono disponibili e sul mercato da più tempo, che sono state scaricate più spesso e che hanno le migliori valutazioni di affidabilità.

9. Stai navigando in un sito web su una rete Wi-Fi pubblica, ma il tuo programma antivirus non è aggiornato. Quale delle seguenti affermazioni è vera?

a) Il dispositivo collegato alla rete Wi-Fi pubblica è ancora sicuro finché si accede solo a pagine contenenti notizie del proprio paese.
b) La comunicazione via http non può essere intercettata.
c) La comunicazione con i sistemi aziendali tramite VPN è sicura.
d) Nessuna delle affermazioni precedenti è vera.

Risposta corretta: d)

Spiegazione: HTTP è un protocollo di comunicazione utilizzato per la comunicazione tra un server web e un browser. Questo protocollo non protegge la riservatezza dei dati trasmessi; i dati possono essere intercettati. È possibile Infettare il computer anche navigando su siti web legittimi, e la probabilità di infezione è più alta se il proprio antivirus, browser o sistema operativo non è aggiornato. Lo stesso vale per la comunicazione VPN.

10. Quale delle seguenti opzioni aiuta a determinare se un sito di shopping online è affidabile?

a) L'indirizzo del sito web inizia con "https://".
b) C'è un marchio sul sito web che riporta la dicitura "100% sicuro".
c) Fare delle ricerche per verificare se il sito ha una buona reputazione.
d) Osservare il sito web e cercare le recensioni positive dei clienti.

Risposta corretta: c)

Spiegazione: I siti maligni possono anche funzionare su https, e i certificati di sicurezza possono essere facilmente falsificati. Il proprietario del sito web può anche pubblicare delle false recensioni dei clienti. L'opzione migliore è fare un po' di ricerca per verificare che il sito abbia una buona reputazione. La reputazione gioca un ruolo importante quando si fa shopping online. La credibilità del sito web dovrebbe essere sempre una valutazione da tenere in considerazione quando si acquista online.

11. Come vengono messi in atto gli attacchi omografi?

a) Il truffatore sfrutta le somiglianze dei caratteri testuali.
b) Il truffatore invia un allegato infetto.
c) Il truffatore invia la stessa e-mail di phishing a tutti i membri dell'azienda.
d) Nessuna delle precedenti.

Risposta corretta: a)

Spiegazione: Gli aggressori hanno iniziato a usare nuove tattiche per confondere gli utenti. Una di queste sono gli omografi. Un attacco omografo si basa sulla sostituzione di una lettera in un URL con un'altra che sembra molto simile o addirittura identica, ma appartiene ad un alfabeto diverso. L'occhio umano non riconosce la differenza, ma un computer che percepisce ogni carattere con un nome in codice diverso sì.

12. Quale delle seguenti attività di gestione delle password è sicura?

a) Su richiesta, fornire la password al proprio superiore.
b) Conservare la password su carta in una busta, chiusa a chiave nella propria scrivania.
c) Su richiesta, fornire la password al responsabile della sicurezza interna.
d) Scrivere la password su un pezzo di carta e incollarlo sul retro della tastiera.

Risposta corretta: b)

Spiegazione: Una password condivisa con persone non autorizzate non è sicura, indipendentemente dalla sua lunghezza, complessità o altre caratteristiche.

13. In che modo gli utenti possono utilizzare le proprie password all'interno di **NOME AZIENDA**?

a) Nessuna restrizione.
b) Le password devono essere complesse. Gli utenti sono autorizzati ad usare le proprie password di **NOME AZIENDA** al di fuori di**NOME AZIENDA**.
c) Le password devono essere complesse. Gli utenti non sono autorizzati ad usare le le proprie password di **NOME AZIENDA** al di fuori di**NOME AZIENDA**.
d) Le password devono essere complesse. Gli utenti sono autorizzati a condividere le password con i propri colleghi.

Risposta corretta: c)

Spiegazione: Gli impiegati devono creare password complesse che siano abbastanza lunghe e non indovinabili da un aggressore. Ci sono diversi approcci per creare una password sicura. Uno è quello di ricordare una frase, ad esempio, "Ho bisogno di cinque caffè per consegnare il codice oggi", e poi cambiare le parole in numeri o caratteri speciali e/o selezionare la prima/seconda/ultima lettera di ogni parola: "Ho bisogno di cinque caffè per consegnare il codice oggi" → "Ho bisogno di 5 caffè x consegnare il c0d1c3 oggi" → "Hbd5cxcico" Il metodo di creazione della password, così come la frase stessa, dovrebbe essere noto solo all'utente della password. Una password usata da un dipendente per accedere ai sistemi informativi (IS) all'interno dell'azienda non deve essere usata per accedere ai IS al di fuori dell'azienda. Non condividere la propria password con NESSUNO: non con i colleghi; non con i familiari, con il responsabile o con il team IT. La propria password non va rivelata a nessuno, nemmeno quado si è in vacanza e qualcuno ha urgente bisogno di accedere al sistema. È il team IT a dover gestire queste situazioni.

14. Ricevi una chiamata e l'interlocutore richiede informazioni sensibili. Come si dovrebbe rispondere?

a) Chiedere all'interlocutore di inviare la richiesta tramite un'email firmata da un indirizzo aziendale e verificarne l'identità.
b) Insistere che lo richiamerai al suo telefono.
c) Chiedere il nome del suo responsabile prima di assecondare la richiesta.
d) Soddisfare la richiesta, dato che ora lavorano da casa e non hanno accesso a un telefono aziendale.

Risposta corretta: a)

Spiegazione: Il vishing è una tipologia di ingegneria sociale telefonica con lo scopo di ottenereinformazioni personali o sensibili da un utente o costringerlo ad eseguire determinate azioni - ad esempio, installare un software di gestione remota per permettere a un "tecnico" di riparare il computer. Si dovrebbe chiedere all'interlocutore di inviare qualsiasi richiesta di informazioni sensibili tramite un'email firmata da un indirizzo aziendale, e prima di rispondere, si dovrebbe verificarne l'identità. Se la persona fornisce un numero a cui essere richiamato o il numero del suo responsabile, potrebbe far parte della truffa - quindi non usarlo. Piuttosto, cerca il numero pubblico ufficiale della società e chiama.

15. Qual è il modo migliore per proteggere la riservatezza dei dati memorizzati su un portatile nel caso in cui questo venga rubato?

a) Crittografia completa del disco.
b) Antifurto.
c) Antivirus.
d) Backup.

Risposta corretta: a)

Spiegazione: Il modo migliore per proteggere la riservatezza dei dati su un computer portatile è la crittografia completa del disco. L'antifurto può aiutare a localizzare il portatile e a recuperarlo, ma il ladro può accedere ai dati sul disco rigido se non è criptato. Una soluzione antimalware non aiuta in caso di furto fisico. Il backup è un mezzo per fornire la disponibilità dei dati, non la loro riservatezza.

16. Posso caricare, archiviare ed elaborare dati aziendali riservati in un servizio cloud non autorizzato (Google Docs, Translate, Drive; Dropbox)?

a) Sì.
b) No.

Risposta corretta: b)

Spiegazione: Le informazioni riservate possono essere memorizzate ed elaborate solo da un fornitore di servizi cloud autorizzato da NOME AZIENDA IT. Categorie speciali di dati confidenziali non possono essere trattate nemmeno da servizi cloud autorizzati.

17. Quali informazioni non dovrebbero essere pubblicate su un profilo social privato? Selezionare tutte le risposte applicabili.

a) Informazioni sulle operazioni interne aziendali
b) Email aziendali e altre informazioni di contatto.
c) Storie divertenti su cose fatte in vacanza.
d) Le proprie informazioni personali, come l'indirizzo e il codice fiscale.

Risposte corrette: a), b), d)

Spiegazione: Informazioni sulle operazioni interne dell'organizzazione,e-mail aziendali e altre informazioni di contatto, e informazioni personali, come l'indirizzo e il codice fiscale, sono informazioni sensibili, e non è opportuno divulgarle.

18. Perché si deve bloccare lo schermo del proprio dispositivo quando non è in uso?

a) Per evitare che un codice maligno si installi automaticamente.
b) Per evitare che persone non autorizzate possano sfruttare i diritti di accesso per accedere ai dati sul dispositivo.
c) Per eseguire correttamente il backup dei dati dal dispositivo.
d) Per rispettare la legge sul copyright.

Risposta corretta: b)

Spiegazione: Una persona non autorizzata può accedere a un dispositivo che non è stato bloccato nella stessa misura del legittimo utente, non viene cioè richiesto l'inserimento di un PIN o di una password per poter continuare a funzionare. Questo significa che un impostore potrebbe ottenere l'accesso a tutti i dati memorizzati su quel dispositivo.

19. Scegli quale opzione NON è una buona pratica di sicurezza fisica.

a) In caso di un'interruzione del lavoro, i dipendenti sono obbligati a bloccare i dispositivi ed eseguire nuovamente l'accesso alla ripresa.
b) I dipendenti sono obbligati a rispettare i principi di *clear desk* (scrivania ordinata) e *clear screen* (schermo ordinato).
c) I dipendenti hanno l'obbligo di effettuare la manutenzione e le riparazioni dei dispositivi aziendali.
d) I dipendenti non devono visualizzare informazioni sensibili in aree in cui persone non autorizzate possano vederle.

Risposta corretta: c)

Spiegazione: Le linee guida in tal senso raccomandano che quando si smette di lavorare con il proprio dispositivo, lo si metta in uno stato in cui sarà necessario effettuare il login alla ripresa del lavoro; si aderisca ai principi di *clear desk* e *clear screen*; e non vengano visualizzate informazioni sensibili in ambienti in cui persone non autorizzate possano vedere i dati visualizzati. Al contrario, la manutenzione e le riparazioni dei dispositivi aziendali sono eseguite esclusivamente da personale di servizio autorizzato e non devono essere effettuate dal dipendente.

Da oltre 30 anni, ESET® è leader nello sviluppo di software e servizi di sicurezza IT per proteggere aziende e utenti finali in tutto il mondo. Con soluzioni che spaziano dalla sicurezza di endpoint e dispositivi mobili, alla crittografia e all'autenticazione a due fattori, i prodotti ESET offrono prestazioni elevate e sono facili da usare, proteggono e monitorano in modo discreto 24/7 i propri clienti, aggiornando le difese in tempo reale per mantenere gli utenti al sicuro ed evitare interruzioni alle attività aziendali. Per maggiori informazioni visita www.eset.com/it/.