SANS SECURITY AWARENESS

Guida operativa alla sicurezza informatica – Lavorare da casa in modo sicuro

Finalità della guida

L'emergenza Coronavirus sta mettendo molte organizzazioni di fronte alla necessità di far lavorare il personale da casa. Questo può risultare molto impegnativo, in quanto spesso non dispongono delle procedure, delle tecnologie e della formazione di cui c'è bisogno per gestire il lavoro a distanza in modo sicuro. Inoltre, molti dipendenti possono ritrovarsi impreparati o disorientati all'idea di dover lavorare da casa. Questa guida vuole aiutarti a formare rapidamente il personale affinché possa lavorare da casa in sicurezza. Se hai qualche domanda sull'uso di questa guida, contattaci all'indirizzo support@sans.org.

Poiché il personale sta attraversando un periodo di forte stress e cambiamenti, a cui si somma una probabile carenza di tempo e risorse a disposizione dell'organizzazione, questa guida vuole rendere la formazione più semplice possibile. Ti suggeriamo di concentrarti sui rischi più gravi e che possono avere un impatto maggiore, tutti descritti qui di seguito. Considerali come un punto di partenza. A questi puoi aggiungere altri rischi o argomenti che ritieni importanti. Però tieni conto che più comportamenti, procedure e tecnologie imponi al personale, più risulta difficile implementarli tutti quanti.

Come utilizzare questa guida

Ti consigliamo di iniziare leggendo questa guida e consultando i collegamenti ai materiali forniti, per farti un'idea di tutte le risorse disponibili. Per ogni rischio vengono proposti vari materiali che puoi usare per formare e sensibilizzare la tua organizzazione. In questo modo puoi scegliere le modalità che ritieni più adatte alle tue esigenze e conoscenze. Dopo aver letto per intero questa guida, consulta anche il Modello per le comunicazioni e la Scheda informativa inclusi in questo kit per adottare una strategia ancora più efficace. Quando hai preso confidenza con tutta la documentazione, ci sono due reparti chiave con i quali devi coordinarti.

1. **Addetti alla sicurezza**: consulta gli addetti alla sicurezza per individuare con precisione i rischi principali che stai cercando di affrontare. In questa guida descriviamo i rischi che secondo noi sono i più importanti e comuni per il personale che lavora da casa, ma nel tuo caso potrebbero essere diversi. Una raccomandazione: spesso gli addetti alla sicurezza commettono l'errore di voler gestire ogni tipo di rischio, sovraccaricando il personale di politiche e requisiti. Meglio limitare al massimo il numero di rischi che si vogliono affrontare. Dopo aver individuato e dato la priorità a questi rischi principali, definisci i comportamenti da adottare per la loro corretta gestione. Come già detto, è probabile che la tua organizzazione abbia carenza di tempo e risorse, perciò attieniti alle indicazioni di base riportate in questa guida.

2. **Addetti alle comunicazioni**: dopo aver individuato i principali rischi umani e i comportamenti più adatti per farvi fronte, collabora con gli addetti alle comunicazioni per formare e sensibilizzare il personale. I programmi più efficaci in tema di sicurezza informatica, infatti, prevedono una stretta collaborazione con gli addetti alle comunicazioni. Se possibile, conviene assegnare uno di questi specialisti anche al reparto degli addetti alla sicurezza. Quando comunichi con il personale, puoi sensibilizzarlo enfatizzando il fatto che questa formazione è utile non solo per lavorare in sicurezza, ma anche per creare un ambiente domestico più sicuro per sé e i propri familiari.

In definitiva, la collaborazione con questi due reparti devi mirare a rendere il tema della sicurezza più chiaro possibile e a motivare il personale, due fattori essenziali per la modifica dei comportamenti. Valuta anche la creazione di un comitato di consulenti che possano darti consigli e riscontri utili sulla gestione del programma. Oltre agli addetti alla sicurezza e alle comunicazioni, vale la pena collaborare e coordinarsi anche con altri reparti, per esempio quello legale o delle risorse umane.

Pacchetto Download Digitale MGT433

SANS Institute offre il corso di formazione di due giorni MGT433 - Come creare, gestire e valutare un programma sulla sicurezza informatica ad alto impatto. Questo corso intensivo delinea tutte le basi teoriche, le competenze, le strutture e le risorse necessarie per creare un programma di formazione ad alto impatto che permetta di gestire e valutare il rischio umano in modo efficace. Come parte di questa guida, rendiamo disponibili i modelli e le risorse di pianificazione inclusi nel Pacchetto Download Digitale del corso. Pur non essendo strettamente necessari ai fini di questa iniziativa, sono materiali che possono risultare preziosi per le organizzazioni più grandi o i programmi più complessi.

Rispondere alle domande del personale

Oltre a comunicare e a formare il personale, è importante utilizzare forum o altri strumenti tecnologici per rispondere agli eventuali dubbi delle persone, meglio se in tempo reale. Per esempio, puoi usare indirizzi e-mail dedicati, aprire canali chat su Skype o Slack oppure creare una specie di social network aziendale con Yammer. Un'altra idea è quella di programmare un webcast sulla sicurezza da ripetere più volte al giorno, per consentire alle persone di seguirlo in diretta all'ora che preferiscono e di porre addirittura delle domande. L'obiettivo di fondo è quello di rendere il tema della sicurezza più accessibile a tutti e risolvere più dubbi possibili. Questa è anche una splendida occasione per motivare il personale e dare un volto più "umano" alla sicurezza, perciò approfittane. Ricorda che tutto questo implica l'assegnazione di risorse per monitorare i canali di comunicazione dedicati alla sicurezza e rispondere attivamente alle domande.

Rischi e materiali di supporto

Abbiamo individuato tre rischi di base ai quali è esposto il personale che lavora da casa. Pur essendo soltanto dei punti di partenza, sono quelli più importanti da considerare. Per ogni rischio riportiamo dei collegamenti a varie risorse che possono aiutare la comunicazione e la formazione sull'argomento. Scegli i materiali che ritieni più efficaci per il tuo caso specifico. Inoltre, quasi tutti i materiali sono disponibili in varie lingue. Se tutto questo risulta troppo impegnativo e hai pochissimo tempo a disposizione, ti suggeriamo di limitarti alle due risorse indicate qui sotto.

1. Scheda informativa Lavorare da casa in modo sicuro (inclusa nel kit operativo)
2. Video Creare una rete domestica sicura (inglese) disponibile anche in altre lingue qui

Ingegneria sociale

Tra i maggiori rischi a cui il personale che lavora da casa va incontro, specie nell'attuale contesto di grandi stravolgimenti ed emergenze, ci sono gli attacchi di ingegneria sociale. Questi attacchi fanno leva sulla sfera emotiva delle persone, che vengono ingannate o raggirate dai criminali informatici affinché commettano uno sbaglio, cosa ancora più facile in questi giorni convulsi. Per questo è importante spiegare alle persone che cosa sono gli attacchi di ingegneria sociale, come si riconoscono e come comportarsi quando se ne individua uno. Non bisogna soffermarsi soltanto sugli attacchi di phishing via e-mail, perché questi attacchi possono avvenire anche tramite telefonate, messaggi, social network o fake news. Trovi tutti i materiali necessari per la formazione e la sensibilizzazione sull'argomento nella nostra cartella Materiali di supporto - Ingegneria sociale. Inoltre, puoi fare riferimento a due video sulla sicurezza informatica di SANS, anch'essi disponibili in varie lingue.

- Ingegneria sociale (inglese) disponibile anche in altre lingue qui
- Phishing (inglese) disponibile anche in altre lingue qui

Password sicure

Come confermato nell'annuale DBIR di Verizon, le password inefficaci continuano a essere tra le principali cause di violazioni della sicurezza. Le quattro precauzioni riportate qui sotto aiutano a contenere il rischio. I materiali che ti servono per formare e sensibilizzare il personale sull'argomento e su queste quattro linee guida si trovano nella nostra cartella Password.

- Passphrase (va notato che complessità delle password e scadenza delle password sono due concetti superati)
- Password univoche per tutti gli account
- Gestori di password

- MFA (Multi-Factor Authentication, "autenticazione a più fattori"). Chiamata anche autenticazione a due fattori o verifica in due passaggi

Sistemi aggiornati

Il terzo rischio riguarda la versione del sistema operativo, dei programmi e delle app per dispositivi mobili usata dalle apparecchiature del personale, che deve essere sempre la più recente e aggiornata. Per coloro che usano dispositivi personali, potrebbe essere necessario attivare gli aggiornamenti automatici. I materiali che ti servono per formare e sensibilizzare il personale sull'argomento si trovano nelle cartelle Malware o Creare una rete domestica sicura.

Ulteriori argomenti da considerare

- **Wi-Fi**: come mettere in sicurezza il punto di accesso Wi-Fi. Questo argomento è trattato nei materiali Creare una rete domestica sicura, ma puoi anche guardare il video Creare una rete domestica sicura (inglese) disponibile anche in altre lingue qui.

- **VPN**: che cos'è una VPN e perché dovresti usarne una. Ti consigliamo di leggere la newsletter OUCH sulle VPN.

- **Lavorare a distanza**: suggerimenti per chi lavora a distanza ma NON da casa, per esempio da bar, terminal degli aeroporti o hotel. È utile guardare il video di training Lavorare a distanza (inglese) disponibile anche in altre lingue qui.

- **Bambini/Ospiti**: per ribadire il fatto che familiari/ospiti non devono avere accesso ad alcun dispositivo di lavoro, guarda il video di training Lavorare a distanza (inglese) disponibile anche in altre lingue qui.

- **Rilevazione/Reazione**: vuoi che le persone segnalino qualsiasi incidente che sospettano si sia verificato mentre lavoravano da casa? In tal caso, quali dettagli devono fornire e quando devono farlo? Tutto questo è trattato nei nostri materiali Vittima di hacker.

Newsletter OUCH

Per potenziare il tuo programma puoi anche avvalerti delle newsletter OUCH disponibili pubblicamente in più di venti lingue. Qui di seguito elenchiamo le newsletter OUCH più utili per la tua iniziativa Lavorare da casa in modo sicuro. Puoi trovare tutte le newsletter negli Archivi delle newsletter sulla sicurezza informatica OUCH disponibili online.

GENERICHE

Four Steps to Staying Secure (Quattro semplici passaggi per la tua sicurezza)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Come creare una casa cyber sicura)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

INGEGNERIA SOCIALE

Social Engineering (Ingegneria sociale)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Attacchi di messaggistica / Smishing)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Truffe targettizzate)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Truffa del CEO)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Truffe telefoniche)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Basta con questi Phish!)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Truffe sui Social Media)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

PASSWORD

Making Passwords Simple (Creazione di password semplici)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Proteggi il tuo Accesso)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

AGGIUNTIVE
Yes, You Are a Target (Sì, sei un bersaglio!)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Dispositivi Smart Home)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Suggerimenti rapidi

Ecco un breve prontuario dei suggerimenti più utili.

- Le misure più efficaci per mettere in sicurezza la rete wireless domestica sono: cambiare la password da amministratore predefinita, attivare la crittografia WPA2 e impostare una password sicura per la rete wireless.
- Prendi nota di tutti i dispositivi connessi alla tua rete domestica, inclusi baby monitor, console di videogiochi, TV, elettrodomestici e perfino la tua automobile. Controlla che tutti questi dispositivi siano protetti da una password efficace e/o che utilizzino la versione più recente del proprio sistema operativo.
- Uno dei modi più efficaci per proteggere il computer a casa è verificare che la versione del sistema operativo e dei programmi sia la più recente e aggiornata. Se possibile, attiva gli aggiornamenti automatici.
- In definitiva, il buonsenso è la tua difesa migliore. Se e-mail, telefonate o messaggi online ti sembrano strani, sospetti o inverosimili, potrebbe trattarsi di un attacco.
- Assicurati di usare password diverse per ognuno dei tuoi account. Non riesci a ricordare tutte le tue password/passphrase? Usa un gestore di password per archiviarle tutte in modo sicuro.
- La verifica in due passaggi è un sistema eccellente per proteggere un account. La verifica in due passaggi richiede, oltre alla password, l'inserimento di un codice generato dal tuo dispositivo mobile o inviato a esso. La verifica in due passaggi è supportata da servizi come Gmail, Dropbox e Twitter.
- Si parla di "phishing" quando un autore di attacchi tenta di indurti con l'inganno a cliccare su un collegamento malevolo o ad aprire l'allegato di un'e-mail. Diffida sempre

quando un'e-mail o un messaggio online crea un forte senso di urgenza, contiene numerosi refusi o si apre con un'espressione generica come "Gentile cliente".

Misurazioni

Le attività di misurazione dei comportamenti sono più difficili da eseguire quando il personale lavora da casa. Inoltre, alcuni di questi comportamenti (come la protezione del proprio dispositivo Wi-Fi) non sono strettamente legati al lavoro. Tuttavia, è possibile misurare il livello di motivazione. Abbiamo valutato che argomenti che toccano anche la sfera personale o emotiva possono destare molto più interesse e aumentare la motivazione. Di conseguenza, i seguenti metodi di misurazione possono tornare utili.

- **Interazioni**: con quale frequenza le persone fanno domande, inviano suggerimenti o chiedono assistenza tramite i canali o i forum sulla sicurezza che hai messo a disposizione?
- **Simulazioni**: prova a organizzare qualche attacco di ingegneria sociale simulato, per esempio tramite e-mail/messaggi di phishing o telefonate fasulle.

Per un elenco dettagliato di tutte le possibili misurazioni, scarica il documento Security Awareness Metrics Matrix incluso nel Pacchetto Download Digitale MGT433.

Licenza

Informazioni sull'autore del kit operativo

Lance Spitzner vanta oltre 20 anni di esperienza nel campo della sicurezza informatica, dallo studio delle minacce informatiche alla progettazione dei sistemi fino ai corsi di formazione sulla sicurezza. Ha contribuito all'avanzamento delle ricerche focalizzate su tecniche di inganno e intelligenza artificiale con la creazione delle "honeynet" e la fondazione di Honeynet Project. Nel ruolo di docente SANS ha sviluppato i corsi MGT433 - Sicurezza informatica e MGT521 - Cultura della sicurezza. Inoltre, Spitzner ha pubblicato tre libri sulla sicurezza informatica, è stato consulente in oltre 25 paesi e ha aiutato più di 350 organizzazioni a creare programmi di sensibilizzazione e promozione della sicurezza per gestire il rischio umano. Spitzner conta numerose apparizioni pubbliche, è un grande utilizzatore di Twitter (@lspitzner) e collabora con numerosi progetti comunitari sulla sicurezza. Prima di dedicarsi alla sicurezza informatica, Spitzner ha servito nella Forza di Dispiegamento Rapido dell'Esercito come Armor Officer e si è laureato in Economia e Commercio all'Università dell'Illinois.

Informazioni su SANS Institute

SANS Institute è attivo dal 1989 nel campo dell'istruzione e della ricerca cooperativa. SANS è il più affidabile e di gran lunga il maggiore fornitore di corsi di formazione e certificazioni in tema di sicurezza informatica rivolti ai professionisti di istituzioni pubbliche e aziende di tutto il mondo. I rinomati docenti SANS organizzano oltre 60 corsi in più di 200 eventi di formazione sulla sicurezza informatica, disponibili anche online. GIAC, affiliata di SANS Institute, verifica le qualifiche dei professionisti mediante 35 certificazioni in sicurezza informatica che prevedono prove pratiche e tecniche. Il SANS Technology Institute, una sussidiaria indipendente con accredito regionale, offre master specialistici in sicurezza informatica. SANS fornisce una vasta gamma di risorse gratuite alla community degli esperti

in sicurezza informatica, tra cui progetti in collaborazione, ricerche e newsletter. Gestisce anche l'Internet Storm Center, un sistema di allarme per le attività online. Al centro di SANS ci sono numerosi professionisti nel campo della sicurezza provenienti da aziende, università e altre grandi organizzazioni globali, che collaborano per supportare l'intera community della sicurezza informatica. (https://www.sans.org)