SANS SECURITY AWARENESS

Ghid de implementare a cunoștințelor despre securitate – Să lucrăm de acasă în siguranță

Rezumat pentru managementul superior

Ca urmare a epidemiei de infecții cu coronavirus, personalul multor organizații ajunge să lucreze de acasă. Acest lucru poate fi o problemă, pentru că multe organizații nu au politicile, tehnologia și calificarea necesare pentru ca oamenii să lucreze în siguranță de acasă. În plus, mulți angajați pot fi neinițiați sau reticenți față de ideea de a lucra de acasă. Acest ghid își propune să vă traseze propune să vă ajute să vă instruiți rapid oamenii să lucreze în condiții de securitate cât mai bune. Dacă aveți întrebări despre utilizarea acestui ghid, contactați-ne la adresa support@sans.org.

Este foarte probabil ca personalul să se confrunte cu mult stres și cu multe schimbări. De asemenea, este probabil ca organizația să aibă de făcut față unor restricții de timp și de resurse. Drept urmare, acest ghid strategic pune accentul pe simplitate. Vă recomandăm să vă concentrați asupra celor mai importante riscuri, care pot avea cele mai puternice efecte, conform descrierii de mai jos. Gândiți-vă la acestea ca la un punct de pornire. Dacă aveți de adăugat alte riscuri sau subiecte, adăugați-le fără să stați pe gânduri. Țineți cont, însă, de următorul fapt: cu cât impuneți personalului mai multe acțiuni, procese sau tehnologii, cu atât scade probabilitatea să le poată adopta pe toate.

Cum se folosește acest ghid

Vă recomandăm să citiți acest ghid și să consultați linkurile la diferitele materiale, ca să vă faceți o idee despre posibilități. Veți observa că la fiecare risc luat în discuție propunem diferite materiale pe care le puteți folosi pentru a mobiliza și a instrui membrii organizației. Drept urmare, puteți selecta modalitățile pe care le percepeți drept cele mai potrivite pentru necesitățile și cultura organizației. După ce ați terminat de citit acest document, citiți Șablonul însoțitor și Fișa de informații din kit, pentru a înțelege mai bine ceea ce încercați să obțineți. După ce ați parcurs documentația, trebuie să vă cooperați cu două grupuri esențiale.

1. **Echipa de securitate**: discutați cu echipa de securitate pentru a înțelege mai bine riscurile cheie pe care încercați să le gestionați. În acest ghid am identificat riscurile pe care le considerăm cele mai importante și mai răspândite în contextul lucrului de acasă. Este posibil ca dvs. să vă confruntați cu alte riscuri. Trebuie să avertizăm că multe echipe de securitate fac o greșeală: încearcă să gestioneze toate riscurile și copleșesc oamenii cu politici și cerințe. Încercați să rezolvați cât mai puține riscuri, doar cele esențiale. După ce le-ați identificat și le-ați stabilit prioritățile, confirmați interacțiunile cu care se vor combate riscurile respective. După cum am menționat deja, dacă organizația dvs. nu are timp sau resurse pentru așa ceva, folosiți aspectele pe care le-am documentat noi în cele ce urmează.

2. **Comunicare**: după ce ați identificat principalele riscuri legate de componenta umană și acțiunile cheie cu care se pot combate acestea, colaborați cu echipa de comunicare pentru a motiva și a instrui personalul să le pună în aplicare. Cele mai eficiente programe de sensibilizare în probleme de securitate au la bază un parteneriat puternic cu echipa de comunicare. Dacă este posibil, încercați să cooptați pe cineva de la comunicare în echipa de securitate. Atunci când comunicați cu forța de muncă, o puteți motiva eficient subliniind faptul că această instruire nu le asigură securitatea doar la serviciu, ci îi ajută și acasă, să-și protejeze căminul și familia împotriva infractorilor cibernetici.

În esență, cooperarea cu aceste două grupuri este menită să simplifice problematica securității (în limita posibilităților) și să motiveze personalul, acestea fiind două elemente esențiale ale schimbărilor comportamentale necesare. Vă recomandăm chiar să creați un Consiliu Consultativ, din care să facă parte persoanele cheie, de ale căror păreri aveți nevoie pentru a implementa programul. În afară de echipele de securitate și de comunicare, este bine să implicați și departamente ca Resurse umane și Juridic.

Pachet de materiale digitale de descărcat MGT433

SANS Institute oferă cursul de instruire MGT433: Cum se creează, se întreține și se măsoară un program de sensibilizare în probleme de securizare care să aibă efecte semnificative. Acest curs intensiv prezintă toate aspectele teoretice, aptitudinile, cadrele și resursele necesare creării unui program de sensibilizare care să aibă efectele scontate, care să vă ajute să gestionați și să măsurați eficient factorii de risc uman. În acest ghid oferim acces la Pachetul de materiale digitale de descărcat, cu șabloane și resurse de planificare. Probabil că materialele sunt mai cuprinzătoare decât ar fi necesar în această inițiativă, dar pot fi valoroase pentru organizațiile mai mari sau pentru implementările mai complexe.

Răspunsuri la întrebările lucrătorilor

În afară de comunicarea cu forța de muncă și instruirea acesteia, recomandăm cu tărie să folosiți o tehnologie sau un forum prin care să puteți răspunde la întrebările oamenilor, preferabil în timp real. Se poate folosi un alias de e-mail, Skype, un canal de chat Slack sau un forum online, cum ar fi Yammer. O altă idee ar fi să găzduiți un webcast despre securitate, pe care să-l repetați de mai multe ori pe săptămână, ca oamenii să poată participa atunci când au timp, eventual să pună și întrebări. Obiectivul este ca securitatea să fie ceva cât mai abordabil și să răspundeți la întrebările oamenilor. Aceasta este o ocazie extraordinară să discutați direct cu lucrătorii și să prezentați securitatea în lumină favorabilă. Încercați să profitați de ea. Nu uitați: aceste eforturi vor da rezultate numai dacă alocați resurse care să modereze canalele de securitate și să răspundă la întrebări.

Riscuri și materiale de instruire

Am identificat trei riscuri esențiale pe care trebuie să gestionați pentru cei care lucrează de la distanță. Acestea constituie un punct de plecare, probabil că sunt aspectele cele mai importante pentru dvs. La fiecare risc prezentat mai jos aveți linkuri la mai multe resurse care vă ajută să comunicați despre subiect și să instruiți oamenii. Oferim mai multe materiale de comunicare, puteți să le alegeți pe cele care vor avea influență optimă asupra culturii organizației. În plus, aproape toate materialele sunt disponibile în mai multe limbi. Dacă găsiți aceste resurse copleșitoare și nu prea aveți timp, vă recomandăm să alegeți și să folosiți cele două materiale menționate mai jos.

1. Fișa de informații Să lucrăm de acasă în siguranță (inclusă în Kitul de implementare).
2. Videoclipul Crearea unui mediu casnic protejat împotriva atacurilor cibernetice (engleză) este disponibil și în alte limbi, aici

Ingineria socială

Unul dintre cele mai importante pericole cu care se confruntă angajații care lucrează de la distanță, în special în aceste vremuri de schimbări dramatice și urgențe, îl reprezintă atacurile de inginerie socială. Ingineria socială este un atac psihologic, în care infractorul păcălește victima să facă o greșeală, ceea ce este mai ușor în perioade de schimbări și confuzie. Cheia este instruirea: oamenii trebuie să știe ce este ingineria socială, cum se identifică principalele semne ale atacurilor de acest tip și ce trebuie făcut în asemenea situații. Aveți grijă să nu abordați doar atacurile de phishing prin e-mail, ci și alte metode, ca apelurile telefonice, SMS-urile, rețelele de socializare și dezinformarea. În folderul Materiale despre ingineria socială veți găsi mai multe materiale de curs legate de acest subiect. În plus, iată două videoclipuri SANS cu informații despre securitate pe care le puteți folosi. Și acestea sunt traduse în mai multe limbi.

- Ingineria socială (engleză), disponibil în alte limbi aici
- Phishing (Engleză), disponibil în alte limbi aici

Parolele puternice

Verizon DBIR, care se face anual, a stabilit că parolele simple sunt în continuare unul dintre principalii factori care favorizează pirateria informatică în lume. Acest risc se poate gestiona prin adoptarea celor patru comportamente cheie prezentate mai jos. Materialele cu care puteți preda și consolida noțiunile legate de acest subiect și de cele patru comportamente cheie se găsesc în folderul Parole.

- Fraze de acces (atenție: atât complexitatea, cât și expirarea parolelor aparțin trecutului).
- Parolă diferită pentru fiecare cont
- Manageri de parole

- Autentificarea prin mai mulți factori (MFA, Multi-Factor Authentication). Numită și autentificare cu doi factori sau verificare în doi pași

Sisteme actualizate

Al treilea risc se leagă de asigurarea instalării celor mai recente versiuni de sisteme de operare și aplicații pe fiecare computer și dispozitiv mobil folosit de angajați. În cazul persoanelor care folosesc dispozitive personale acest lucru poate presupune activarea actualizării automate. Materialele necesare predării și consolidării acestor noțiuni se găsesc în folderele Programe rău intenționate și Crearea unui mediu casnic protejat împotriva atacurilor cibernetice.

Subiecte suplimentare de luat în considerare

- **Wi-Fi**: securizarea punctului de acces Wi-Fi. Acest subiect este prezentat în materialele Crearea unui mediu casnic protejat împotriva atacurilor cibernetice. Vă ajută și Videoclipul Crearea unui mediu casnic protejat împotriva atacurilor cibernetice (engleză), disponibil în alte limbi aici.

- **VPN**: ce este și de ce să folosiți VPN. Vă recomandăm Buletinul informativ OUCH despre VPN.

- **Lucrul de la distanță**: Aici este vorba despre persoanele care lucrează de la distanță, dar NU de acasă, de exemplu, dintr-o cafenea, un aeroport sau un hotel. Puteți folosi Videoclipul de instruire Lucrul de la distanță (engleză), disponibil în alte limbi aici.

- **Copii / vizitatori**: Pentru a accentua ideea că membrii familiei și vizitatorii nu trebuie să aibă acces la dispozitivele de lucru, folosiți Videoclipul de instruire Lucrul de la distanță (engleză), disponibil în alte limbi aici.

- **Detectare / reacție**: Doriți ca oamenii să raporteze dacă bănuiesc că a avut loc un incident în timp ce lucrau de acasă? Dacă da, ce doriți să raporteze și când? Materialele Atacat de hackeri abordează aceste aspecte.

Buletinele informative OUCH

Puteți să vă susțineți programul cu buletinele informative OUCH cu acces public. Fiecare dintre acestea este tradus în peste douăzeci de limbi. Prezentăm în continuare enumerate buletinele informative OUCH pe care le considerăm cele mai utile pentru inițiativa Să lucrăm de acasă în siguranță. Toate buletinele informative se găsesc în Arhiva de buletine informative despre securitate OUCH.

PREZENTARE GENERALĂ

Four Steps to Staying Secure (Patru pași pentru siguranță)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Crearea unui mediu casnic protejat împotriva atacurilor cibernetice)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

INGINERIA SOCIALĂ

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

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

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

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

Phone Call Attacks / Scams (Atacuri / înșelătorii prin telefon)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Opriți atacurile de phishing)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Atacuri prin rețelele de socializare)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

PAROLELE

Making Passwords Simple (Cât mai simplu despre parole)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) [Conectare cu protecție cu suplimentară (2FA)]
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

SUPLIMENTAR

Yes, You Are a Target (Da, sunteți o posibilă victimă)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

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

Sfaturi rapide

Sfaturi și indicații pe care le puteți distribui în format ușor accesibil.

- Cele mai eficiente măsuri pe care le puteți lua pentru a vă securiza rețeaua wireless de acasă sunt modificarea parolei de administrator implicite, activarea criptării WPA2 și utilizarea unor parole puternice în rețeaua respectivă.
- Țineți cont de toate dispozitivele conectate la rețeaua de acasă, inclusiv camerele de supraveghere a bebelușilor, consolele de joc, televizoarele, electrocasnicele și chiar mașina. Asigurați-vă că toate dispozitivele respective sunt protejate prin parole puternice și/sau au cele mai recente versiuni de sisteme de operare.
- Una dintre cele mai eficiente metode de a proteja computerul de acasă este actualizarea sistematică a sistemului de operare și a aplicațiilor. Dacă este posibil, activați actualizarea automată.
- Până la urmă, bunul simț vă asigură cea mai bună protecție. Dacă un e-mail, un mesaj sau un apel telefonic pare ciudat, suspect sau sună prea bine ca să fie adevărat, poate fi un atac.
- Aveți grijă ca fiecare cont pe care îl folosiți să aibă o parolă unică, diferită de celelalte. Nu puteți reține toate parolele/frazele de acces? Le puteți păstra securizat pe toate într-un manager de parole.
- Verificarea în doi pași este una dintre cele mai bune modalități de a securiza orice cont. Vorbim despre verificare în doi pași atunci când se cere atât o parolă, cât și un cod

trimis pe dispozitivul mobil sau generat de acesta. Exemple de servicii care folosesc verificarea în doi pași: Gmail, Dropbox și Twitter.

- Phishingul se referă la încercarea atacatorului de a vă păcăli să faceți clic pe un link nociv sau să deschideți un fișier atașat dintr-un e-mail. Trebuie să vă trezească bănuielile toate e-mailurile și mesajele online care induc un sentiment al urgenței, au ortografie îndoielnică sau vi se adresează cu „Dragă Client”.

Indicatori

Indicatorii comportamentali sunt greu de urmărit în această situație, întrucât este greu de măsurat cum se comportă oamenii acasă. De asemenea, unele dintre aceste acțiuni nu sunt specifice activităților de lucru (de exemplu, securizarea dispozitivelor Wi-Fi). Cu toate acestea, interacțiunile se pot măsura. Am constatat că subiectele personale sau care stârnesc emoții pot fi foarte atrăgătoare și pot atrage mult mai multă atenție decât altele. Drept urmare, indicatorii precum cei de mai jos pot fi foarte utili.

- **Interacțiune**: cât de des pun oamenii întrebări, cât de des postează idei sau cer ajutor prin canalele sau forumurile de securitate pe care le găzduiți?
- **Simulări**: simulați atacuri de inginerie socială, de exemplu, atacuri de phishing, prin SMS sau prin telefon.

Pentru o listă cu mult mai mulți indicatori, descărcați Matricea interactivă cu indicatori ai atenției acordate securității din Pachetul de materiale digitale de descărcat MGT433.

Licență

Autorul Kitului de implementare

Lance Spitzner are peste 20 de ani de experiență în cercetarea amenințărilor cibernetice, în arhitecturile de securitate, în sensibilizare și în instruire. A făcut muncă de pionierat în domeniile combaterii înșelătoriei și a spionajului cibernetic, prin crearea de honeynets și prin lansarea Honeynet Project. În calitate de instructor SANS, a dezvoltat cursurile MGT433: Curs informativ privind securitatea și MGT521: Cultura securității. Mai mult, Lance a publicat trei cărți despre securitate, a fost consultant în peste 25 de țări și a ajutat peste 350 de organizații să creeze programe de sensibilizare și cultură de securitate, pentru gestionarea riscurilor legate de factorul uman. Lance ține multe prezentări, este activ pe Twitter (@lspitzner) și lucrează la multe proiecte de securitate comunitară. Înainte de a se ocupa de securitatea informatică, Dl. Spitzner a fost tanchist în Forțele de intervenție rapidă ale Armatei și a absolvit Universitatea din Illinois.

Despre SANS Institute

SANS Institute a fost înființat în 1989, ca organizație de cercetare și învățământ. SANS este cel mai de încredere și de departe cel mai mare furnizor de cursuri și certificate de cibersecuritate pentru specialiștii din instituțiile publice și comerciale din toată lumea. Instructorii SANS sunt autorități în domeniu și țin peste 60 de cursuri diferite la peste 200 de evenimente de instruire în cibersecuritate, live, dar și online. GIAC, organizație afiliată la SANS Institute, validează calificările cadrelor prin peste 35 de examene tehnice, cu probe practice de certificare în cibersecuritate. SANS Technology Institute, o filială independentă cu acreditare regională, oferă masterate în cibersecuritate. SANS pune la dispoziția comunității InfoSec o mulțime de resurse gratuite, inclusiv proiecte de consens, rapoarte de cercetare și buletine informative. De asemenea, este operatorul sistemului de avertizare timpurie Internet Storm Center. Esența SANS sunt specialiștii în securitate care reprezintă diferite organizații globale, de la corporații la universități, care cooperează pentru a ajuta întreaga comunitate de securitate informativă. (https://www.sans.org)