Securizarea accesului de la distanță, pentru administratori

Atunci când apar astfel de evenimente de perturbarea severă a interacțiunii sociale, adoptarea unei opțiuni de lucru de acasă este esențială pentru continuitatea afacerii. Dar, pentru a menține angajații productivi și afacerea să funcționeze, implementarea în grabă a acestui tip de mod de lucru poate lăsa organizația dvs. vulnerabilă din punct de vedere al securității. Dacă există un singur lucru pe care îl știm despre infractorii cibernetici este acela că nu vor ezita să profite de noi oportunități. Utilizați această listă de sfaturi pentru a vă ajuta să vă protejați forța de muncă indiferent de locația în care se află.

☐ Îmbunătățiți politicile de setare a parolei

Dacă ați fost relaxați privind acest aspect până acum, situația de față impune îmbunătățirea rapidă a politicilor de setare a parolelor. Solicitați parole lungi (sau mai bine, parole formate din mai multe cuvinte, passphrases), impuneți modificări periodice și blocați conturile după un număr stabilit de autentificări eșuate. Explicați-le angajaților că nu își pot reutiliza parolele de lucru pentru niciunul alt cont personal.

☐ Implementați autentificare multi-factor (MFA)

Cunoscută și sub numele de autentificare în doi factori (2FA), aceasta este cea mai bună metodă de apărare împotriva infractorilor cibernetici care utilizează tehnici de predicție, atacuri de password-spraying sau utilizează credențiale subtilizate anterior și mai apoi achiziționate din dark web pentru a impersona angajații și pentru a se infiltra în rețeaua dvs. Dacă utilizați servicii de e-mail bazate pe cloud, suite de productivitate sau alte aplicații, activați autentificarea MFA dacă este disponibilă.

☐ Solicitați o conexiune VPN pentru accesarea rețelei dvs. interne

Un VPN criptează traficul dvs. corporativ pe măsură ce traversează internetul public, astfel încât acesta să nu poată fi citit de către infractorii cibernetici. În plus, o conexiune VPN permite echipei IT să extindă mai multe măsuri de securitate din rețeaua internă către dispozitivele de la distanță. Dacă utilizați deja un VPN pentru unii angajați, asigurați-vă că aveți suficiente licențe și capacitatea pentru a acoperi noii utilizatori. Dacă angajații vor accesa resurse din rețeaua dvs. internă, combinația dintre VPN și MFA este un lucru imperios necesar.

☐ Utilizați o soluție de interfață desktop virtuală, dacă este posibil

Cu acest tip de soluție, angajatul accesează o mașină virtuală care se află fie în cloud, fie în centrul de date și îl controlează de la distanță. Poate fi configurat să arate exact ca un sistem de lucru obișnuit. Avantajul este că datele sau fișierele sensibile există doar pe mașina virtuală și nu sunt niciodată stocate pe sistemul de acasă al angajatului.

☐ Reamintiți-le angajaților să fie vigilenți la rețeaua de date utilizată, mai ales la Wi-Fi

Un lucru care vă scapă complet de sub control este rețeaua angajaților de acasă și alte dispozitive care se conectează la aceasta. Sfătuiți-i să oprească orice partajare de fișiere pe sistemul pe care îl vor folosi pentru muncă și să verifice router-ul sau punctul de acces Wi-Fi pentru a fi siguri că securitatea WPA2 este activată. Reamintiți-le să nu se conecteze niciodată la un punct de acces Wi-Fi nesecurizat sau deschis care nu necesită o cheie de securitate.

Investiți în securitatea endpoint a angajaților care lucrează de acasă

Nu puteți avea încredere că antivirusul livrat cu un sistem desktop obișnuit sau cu un dispozitiv personal este suficient de capabil. O soluție completă protejează împotriva tuturor tipurilor de amenințări cu mai multe straturi de securitate, inclusiv un firewall personal, protecție împotriva site-urilor web dăunătoare și protecția împotriva malware-urilor de pe unitățile USB portabile. Cea mai bună opțiune aici este o suită de securitate endpoint de tip business pe care departamentul IT să o poată administra de la distanță.

Solicitați o metodă de criptare dacă angajații vor lucra cu fișiere sensibile

Dacă angajații vor descărca fișiere corporative pe dispozitivele lor personale, oferiți-le o soluție de criptare. Insistați să păstreze fișierele personale separate de documentele de lucru și să salveze tot ce este legat de job într-un folder criptat. De asemenea, aplicați o politică prin care se salvează documentele revizuite într-un mediu de stocare corporativ, astfel încât sau nu fie nevoie să vă faceți griji cu privire la backup-ul de la distanță.

Sfătuiți angajații să se deconecteze ori de câte ori iau o pauză

Când angajații își iau pauzele de prânz, termină ziua sau oricând se îndepărtează de dispozitivul lor mai mult de câteva minute, ar trebui să se deconecteze din rețeaua business. Este o practică bună oricând, nu doar în această perioadă. Este obligatoriu dacă dispozitivul este partajat cu alte persoane din familie sau dacă alte persoane din casă îl pot accesa.

Promovați instalarea patch-urilor și a actualizărilor

Comunicați-le angajaților conectați de la domiciliu să permită actualizările automate pe toate sistemele lor, pentru a vă asigura că sunt la zi cu toate măsurile de securitate. Verificați din nou dacă și mediul dvs. intern este actualizat, în special elementele și sistemele critice pentru securitate, care ar putea rămâne neactualizate, deoarece acestea rulează 24/7. Fiți atenți la sistemele angajaților de acasă care rulează Windows 7, căruia nu îi mai este oferit suport. Este posibil să fie nevoie de interziceți accesul până când se face o actualizare la o versiune acceptată.

Oferiți training-uri în domeniul securității cibernetice pentru angajați

Oricât de multe straturi de securitate ați pus în aplicare, o altă protecție importantă constă în oamenii cu care lucrați și mai precis informațiile pe care aceștia le dețin. Notificări false care impersonează entitatea business la care lucrează, care pretind confirmarea datelor de autentificare, vizitarea site-urile care în aparență sunt legitime, primirea de solicitări false de la coordonator pentru a facilita o plată sau un transfer de fonduri, și alte escrocherii de acest tip vor fi în creștere, în timp ce infractorii cibernetici vor încerca să profite de angajații care lucrează de acasă. Angajații informați și cei care sunt vigilenți au șanse mai puține să fie victime. Mai ales atunci când lucrează de la distanță, un program de training regulat îi va menține la un nivel ridicat de conștientizare a problemelor de securitate.

Avem și o veste bună

Suite de securitate anti-malware care pot fi administrate prin consolă cloud, colaborarea online prin chat și alte tehnologii de acces securizat la internet și de la distanță pot face ca angajații să fie fel de productivi de acasă ca atunci când sunt la birou - adesea chiar mai productivi. În momentul în care încep să lucreze de acasă, asigurați-vă că implementați toate măsurile de securitate potrivite.

Pentru mai multe informații despre soluțiile de securitate ESET, vizitați site-ul nostru dedicat