Ghidul administratorului IT pentru securizarea lucrului de la distanță

În vreme ce pandemia forțează mulți angajați să lucreze de acasă, poate compania dvs. să rămână în continuare productivă și totuși în siguranță? Companiile de tehnologie de înalt profil, precum Google și Microsoft, încurajează sau impun ca personalul lor să adopte o politică de lucru de acasă. Cu toate acestea, pentru multe alte companii și organizații mai mici, situația este diferită.

Posibilitatea de a lucra de la distanță este probabil limitată la un număr mic de companii, în principal la cele care se bazează pe comunicarea prin e-mail. Cum să vă asigurați că infrastructura și politicile sunt toate în configurate pentru a asigura continuitatea activității?

Cerințe de bază

În primul rând, pentru a rămâne productivi, există anumite cerințe comune de care au nevoie toți angajații care lucrează de la distanță.

- Un calculator
- O conexiune bună la internet
- Aplicații pentru chat și conferințe
- Un spațiu de lucru dedicat (de preferat)
- Opțional, un telefon
- Auto-motivație și disciplină
- Rutină strictă

Companiile și organizațiile trebuie să se pregătească atât intern, dar să își pregătească angajații și cu privire la **riscurile crescute de securitate cibernetică** asociate cu munca de la distanță.

Care sunt o parte dintre provocările care ar trebui să fie abordate?

1. Securitatea fizică a dispozitivelor companiei
2. Securitatea IT a companiei atunci când angajații lucrează de acasă
3. Ce se află în mediul tehnologic de acasă
4. Accesarea rețelei și sistemelor companiei
5. Instrumente de colaborare și procese de autorizare
6. Pregătire cibernetică
7. Suport tehnic și gestionarea crizelor

1 Securitatea fizică a dispozitivelor companiei

Lucrând de acasă, angajații vor expune sistemele companiei unui risc sporit, pentru că părăsesc siguranța sau securitatea infrastructurii de lucru de la birou. Echipamentele de lucru trebuie însă protejate în acest caz împotriva pierderilor și furtului. Iată câteva măsuri și sfaturi cheie despre cum să vă asigurați că toate dispozitivele rămân securizate.

- **Deconectați-vă din aplicațiile folosite** — atunci când nu folosiți dispozitivul în acest scop, atât acasă, cât și în locurile publice. Situația nedorită în care un copil curios poate trimite accidental un e-mail poate fi evitată cu ușurință, de asemenea, accesul unei persoane străine la informațiile afișate pe ecran este blocat, eliminând orice risc într-un spațiu public..
- **Implementați o politică puternică de parole** — activați parolele la pornirea dispozitivului sau aplicației, setați după ce perioadă de inactivitate să se închidă dispozitivul și nu permiteți ca parolele să fie notate pe hârtie: oamenii continuă să facă acest lucru!
- **Nu lăsați niciodată dispozitivul de lucru nesupravegheat** sau la vedere. Dacă îl transportați în mașină, atunci ar trebui să îl depozitați în portbagaj.

PRO TIP

Criptarea full-disk este o soluție simplă, dar puternică, asigurându-vă că în situația în care laptopurile sunt pierdute sau furate, datele companiei nu sunt compromise.

Securitatea IT a companiei atunci când angajații sunt acasă

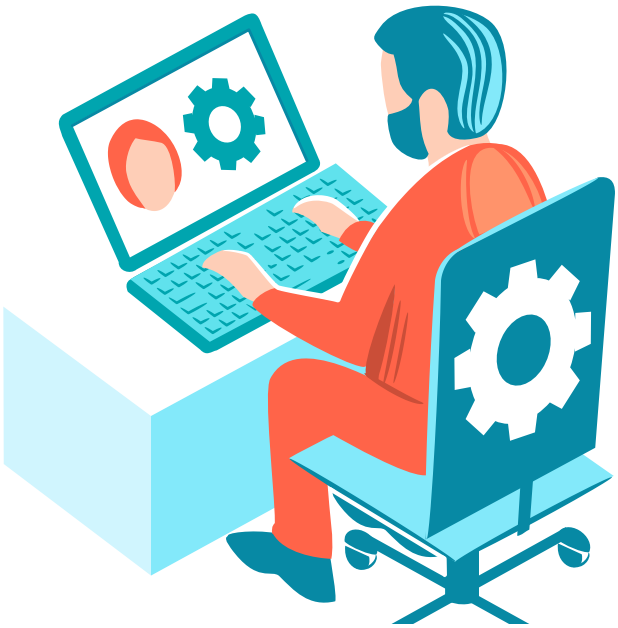
2 Acum că angajații sunt singuri în casele lor, aveți o vizibilitate limitată a ceea ce se întâmplă, mai ales dacă nu sunteți obișnuit să gestionați și să monitorizați echipamentele de lucru de la distanță. Este un moment bun pentru a afla toate avantajele managementului de la distanță pentru a reduce semnificativ numărul de probleme IT pe care va trebui să le gestionați.

Utilizarea managementului la distanță vine cu următoarele avantaje:

- Puteți configura și menține cu ușurință toate sistemele actualizate. Simultan, fără a fi nevoie să repetați procesul pe fiecare dispozitiv.
- Vă ajută să planificați taskuri, să definiți politici și să le executați pe diferite grupuri de angajați.
- Vă transmite în timp real notificări privind incidentele, pentru a putea acționa imediat.

PRO TIP

Dacă aveți până în 250 de dispozitive, puteți gestiona cu ușurință rețeaua de calculatoare prin intermediul unei console cloud. Activarea acesteia durează doar câteva minute.



3 Ce se află în mediul tehnologic de acasă

Cereți angajaților să verifice propriul mediu de lucru împotriva vulnerabilităților, înainte de a conecta dispozitivele de lucru. Apar permanent știri cu privire la vulnerabilitățile echipamentelor IoT (Internet of Things), iar acesta este un moment excelent pentru angajați să ia măsuri privind securizarea acestora cu parole puternice și să actualizeze firmware-ul/software-ul acestora la cele mai recente versiuni disponibile.

Vă puteți sfătui angajații sau chiar le puteți cere să utilizeze o aplicație de monitorizare a dispozitivelor mobile conectate înainte de a integra echipamentele de lucru în rețelele de acasă. Scanarea sau monitorizarea vor evidenția dispozitivele cu vulnerabilități cunoscute, versiunile software sau firmware neactualizate sau utilizarea unor parolelor implicite, care trebuie modificate.

4 Accesarea de la distanță a rețelei și sistemelor companiei

Stabiliți dacă angajatul are nevoie de acces la rețeaua internă a organizației sau doar la serviciile de e-mail din cloud. Și evaluați din nou dacă același nivel de acces la datele sensibile, de care se bucura lucrând din sediu, ar trebui menținut atunci când activitatea angajatului este derulată de la distanță.

Dacă este nevoie de acces la rețeaua internă a organizației:

- Este recomandat ca acest lucru să se realizeze numai cu un echipament deținut de companie, astfel încât controlul complet al dispozitivului de conectare să fie sub conducerea echipei IT.
- Utilizați întotdeauna un **VPN pentru a conecta angajații de la distanță** la rețeaua internă a organizației. Acest lucru împiedică atacurile, care se interpun fluxului de date transmise din locații îndepărtate: nu uitați că, de acum, lucrând de acasă, fluxul de informații circulă prin rețelele publice.
- **Controlați utilizarea dispozitivelor externe,** cum ar fi stocarea USB și dispozitivele periferice.
- Având în vedere că mulți angajați lucrează de acasă, aceștia devin ținte ale campaniilor de scam prin e-mailuri de tip phishing. Puteți **menține la distanță e-mailurile suspecte** cu ajutorul soluțiilor de tip cloud-sandboxing.
- Limitați capacitatea de a stoca, descărca sau copia date. O breșă de date poate avea loc de la nivelul oricărui dispozitiv care stochează date sensibile.
- Luați în considerare utilizarea mașinilor virtuale pentru a oferi acces. Această opțiune poate fi mai greu de configurat, dar ar putea fi o soluție superioară pe termen lung.

În cazul în care o parte (sau toți) angajații dvs. utilizează dispozitive BYOD (personale), dacă le permiteți accesul la servicii de e-mail și cloud, asigurați-vă că aplicați aceeași politică de securitate anti-malware, firewall etc., ca atunci când utilizează un echipament al companiei. **Dacă este necesar, furnizați angajatului o licență similară cu cea utilizată pe dispozitivele deținute de companie.** Dacă aveți nevoie de licențe suplimentare, contactați furnizorul. Este posibil să fie disponibile soluții care să vă protejeze în timpul acestui eveniment fără precedent.

PRO TIP

Autentificarea multifactor (MFA) vă asigură că accesul, fie la serviciile bazate pe cloud, fie la rețea, este realizat numai de către utilizatorii autorizați. Ori de câte ori este posibil, utilizați un sistem de acest tip, bazat pe o aplicație mobilă sau un token fizic, pentru a genera coduri unice care acordă acces autentificat.

5 Instrumente de colaborare și procese de autorizare

Poate părea ciudat să punem împreună aceste două denumiri în același titlu, dar unul poate ajuta la prevenirea problemelor dacă este folosit împreună cu celălalt.

- Oferiți acces la sisteme de chat și video-conferință, astfel încât angajații să poată comunica între ei. Sunt instrumentele de productivitate necesare care îi ajută pe angajați să rămână conectați cu ceilalți colegi.
- Instrumentele de colaborare vă pot proteja împotriva instrucțiunilor neautorizate sau tranzacțiilor nesolicitate, comunicate pentru a păcăli angajații. Infractorii cibernetici vor exploata intens oportunitatea pe care o oferă munca de la distanță, pentru a lansa atacuri de tip Business Email Compromise (BEC). Prin intermediul e-mail-ului este trimisă o cerere falsă, cu caracter urgent, în spatele căreia se află un infractor cibernetic, prin care se solicită transferuri și plăți, fără posibilitatea de a valida cererea în persoană.

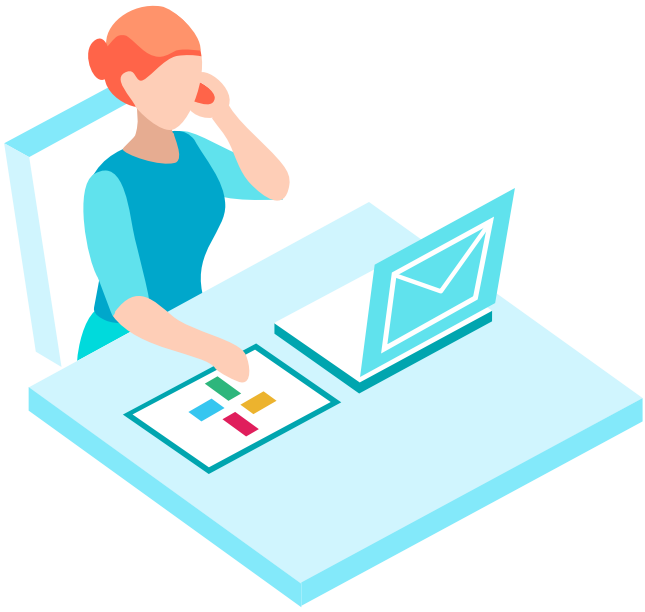
Asigurați-vă prin sisteme de conferință video / chat, ca parte formală a sistemului de aprobare, că orice astfel de validare să se facă „personal", chiar dacă de la distanță.

6 Pregătire cibernetică

Am asistat deja la numeroase escrocherii care exploatează criza provocată de COVID-19, cum ar fi vânzarea de măști de protecție, promisiunea existenței unui vaccin sau informații false menite să dezinformeze. Atunci când angajații sunt mutați de la locul de muncă și sunt plasați într-un loc mai confortabil, ei pot accesa mai ușor astfel de link-uri..

PRO TIP

Cursurile de instruire privind conștientizarea securității cibernetice sunt de obicei o cerință anuală pentru angajați. Mai ales acum, când se lucrează de la distanță, derulați o campanie de instruire și cereți angajaților să parcurgă o astfel de pregătire.



7 Suportul și managementul crizelor

În graba de a oferi acces de la distanță, nu sacrificați securitatea cibernetică sau abilitatea de a gestiona sisteme și dispozitive. Capacitatea de a oferi suport utilizatorilor, de la distanță, va fi esențială pentru a asigura o funcționare fără probleme, mai ales dacă angajații vor rămâne în carantină prelungită. Angajații de la distanță trebuie să aibă protocoale clare de comunicare pentru a cere suport IT și pentru gestionarea crizelor dacă se confruntă cu probleme neobișnuite sau suspecte care ar putea fi rezultatul unei breșe a datelor.

Este ușor să presupunem că toți angajații se pot adapta foarte ușor, la o activitate de la distanță, fără prea mult ajutor. Dar spațiul de acasă nu este același cu biroul, iar unele persoane au nevoie de ajutor pentru a se adapta

Cum vă poate ajuta ESET?

Când discutăm despre securitatea modului de lucru la distanță și de provocările sale, vă puteți baza pe ESET. Iată câteva dintre soluțiile noastre care vă vor ajuta compania să rămână în siguranță și productivă în aceste momente dificile.

MANAGEMENT REMOTE

ESET Cloud Administrator

Securitate bazată pe cloud, pentru până la 250 de stații, care vă ajută să economisiți costuri, timp și simplifică protecției rețelei dvs.

- Configurare și implementare în câteva minute
- Nu este nevoie de hardware sau software suplimentar
- Panou unic de gestionare a securității rețelei
- Accesibil de oriunde, în siguranță, prin intermediul browser-ului

Explorați acum soluția

DISPOZITIVE SECURIZATE

ESET Endpoint Protection

Tehnologie multistratificată, machine learning și expertiză umană, toate aceste caracteristici combinate cu un management

- Protecție ușor de utilizat, oferind administrare de la distanță prin cloud
- Vă protejează de atacuri targetate, de ransomware și de atacuri fileless
- Puteți integra ușor add-on-ul ESET Full Disk Encryption

Explorați acum soluția

ACCES SECURIZAT

ESET Secure Authentication

O metodă simplă și eficientă, pentru companii, de a implementa autentificarea cu multi-factor pe sistemele utilizate în mod obișnuit. Vă permite să:

- Preveniți breșele de date
- Respectați cerințele de conformitate
- Gestionați securitatea în mod centralizat din browser-ul dvs.
- Folosiți ca metodă de verificare telefonul sau token-uri hardware

Explorați acum soluția

Pentru mai multe informații privind soluțiie remote vizitați site-ul nostru