

CERT-RO a elaborat un set de recomandari pentru telemunca

Centrul National de Raspuns la Incidente de Securitate Cibernetica (CER-RO) a elaborat un set de recomandari pentru angajatori si angajati, în cazul în care activitatea se desfasoara în regim de telemunca.

Astfel, expertii în securitate cibernetica îi sfatuiesc pe angajatori sa ofere o politica clara în cazul telemuncii, incluzând ghiduri privind accesarea resurselor companiei, cine este persoana de contact în caz de probleme, sa stabileasca o procedura clara în caz de incidente de securitate si sa aplice masuri suplimentare privind documentatia care va necesita atenta conducerei în scopuri de semnatura, aprobare/feedback si informare.

De asemenea, recomanda implementarea unor masuri de securitate precum criptarea hard disk-ului, timpul de inactivitate, ecranele de protectie, autentificarea complexa, precum si controlul/criptarea mediilor de stocare (ex. stick USB) si implementarea de proceduri pentru dezactivarea de la distanta a accesului la un dispozitiv pierdut sau furat.

Expertii CERT-RO le mai sugereaza angajatorilor sa permita doar angajatilor lor sa se conecteze la reseaua companiei printr-o solutie de tip VPN cu autentificare multi-factor si sa se asigure ca sesiunile la distanta se pot deconecta automat si necesita reautentificare dupa o anumita perioada de inactivitate.

Totodata, actualizarea frecventa a sistemului de operare si a aplicatiilor scade riscul de compromitere a dispozitivelor prin vulnerabilitati nerezolvate.

U alt sfat se refera la securizarea comunicatiilor companiei, prin aplicarea autentificarii multi-factoriale pentru a accesa conturile de e-mail ale companiei.

"Oferiti acces la canale sigure de comunicare între angajati, precum si unele similare pentru comunicarea cu exteriorul", spun expertii în securitate cibernetica.

Alte recomandari se refera la cresterea capacitatii de monitorizare a securitatii, prin verificarea, constant, a activitatilor neobisnuite pe dispozitivele companiei si cresterea nivelului de alerta pentru atacuri legate de VPN, la cresterea nivelului de constientizare al angajatilor în ceea ce priveste riscurile de securitate ale telemuncii si efectuarea de verificari periodice cu personalul.

Pe de alta parte, pe angajati, CERT-RO îi sfatuiesc sa foloseasca doar dispozitive si software furnizat de companie, sa creeze parole puternice si sa evite optiunile de lucru alternative, chiar daca par sa ofere exact ceea ce au nevoie.

Înainte de a începe lucrul de la distanta, acestia trebuie sa se familiarizeze cu dispozitivele, politicile si procedurile companiei si sa se asigure ca înțeleg modul de operare al echipamentelor, ceea ce trebuie facut si ce nu (în cazul acestora) si unde sa se adreseze.

Conectarea la reseaua companiei trebuie sa se faca doar prin VPN si sa fie protejate token-urile (sau cardurile inteligente) necesare pentru conexiunea VPN.

"Protejeaza echipamentul si mediul de lucru la distanta. Nu permiteti membrilor familiei sau altor persoane sa va acceseze dispozitivele de lucru. Blocati-le sau închideti-le când sunt nesupravegheate si pastrati-le întotdeauna într-o locatie sigura, pentru a preveni pierderea, deteriorarea sau furtul. Împiedicati scurgerea de date accidentala, folosind ecrane de confidentialitate si evitati orientarea ecranelor spre ferestre sau camere foto. Daca observati vreo activitate neobisnuita sau suspecta pe orice

dispozitiv pe care îl utilizați pentru a lucra la distanță, contactați imediat angajatorul pe canale sigure. Atenție la orice activități sau cereri suspecte, în special la cele financiare. Ar putea fi o fraudă! În cazul în care aveți dubii, apălați solicitantul pentru a verifica. Nu faceți clic pe linkurile sau fișierele atașate primite în e-mailuri și mesaje text nesolicitate", îi mai sfătuiesc experții pe angajați.

De asemenea, le recomandă acestora să nu răspundă niciodată cu informații personale la mesaje, chiar dacă pretind că provin dintr-o sursă legitimă și să contacteze direct compania pentru a confirma solicitarea acestora.

Planurile de lucru trebuie discutate cu conducerea și membrii echipei, în perioada lucrului de la distanță, inclusiv distribuirea sarcinilor, a termenelor și a canalelor de comunicare.

În cazul în care utilizarea dispozitivului personal este singura opțiune de lucru și angajatorul permite folosirea lui, angajatul trebuie să se asigure că sistemul de operare și software-ul dispozitivului sunt actualizate, există o soluție antivirus instalată, iar conexiunea este securizată printr-un VPN aprobat de companie. Totodată, trebuie evitată folosirea în interes personal a dispozitivelor dedicate lucrului de la distanță.