AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Rekomandime Për Sigurinë Në Internet

Kur Punoni Nga Shtëpia

20/03/2020

Autoriteti Kombetar per Certifikim Eletrokin dhe Sigurine Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Indeksi

Hyrje

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në rolin e CSIRT Kombëtar ka hartuar disa rekomandime kryesore për punën e telekomunikacionit në kohën e Covid-19. Këto rekomandime janë bazuar në udhëzimet e dhëna nga ENISA (Agjencia Kombëtare e Sigurisë se Informacionit Evropian)

Një nga masat kryesore parandaluese për përhapjen e Covid-19 është distancimi social. Për fat të mirë, në këtë botë gjithnjë e më të lidhur mund të vazhdojmë jetën tonë profesionale dhe private në mënyrë virtuale. Sidoqoftë, me rritje të mëdha të numrit të njerëzve që punojnë në distancë, është me rëndësi jetike që të kujdesemi edhe për higjienën tonë në internet.

Rekomandime për punëdhënësit dhe stafin

Rekomandimet e mëposhtme për ruajtjen e një niveli adekuat të sigurisë kibernetik janë ndarë në dy nivele si për punëdhënësit dhe stafin që punojnë nga shtëpia.

Rekomandime për punëdhënësit

- Sigurohuni që zgjidhjet e përshkallëzuara të VPN për korporata të jenë në gjendje të mbajnë një numër të madh të lidhjeve të njëkohshme.
- Siguroni konferenca të sigurta për klientët e korporatave si audio ashtu edhe video.
- Të gjitha aplikimet e biznesit të korporatave duhet të
- jenë të aksesueshme vetëm përmes kanaleve të komunikimit të koduar (SSL VPN, IPSec VPN).
- Aksesi në portalet e aplikacionit duhet të mbrohet duke përdorur mekanizma të shumë faktorëve të autentikimit.
- Parandaloni ekspozimin e drejtpërdrejtë në internet të ndërfaqeve me akses remote në (p.sh. RDP). Autentikimi i ndërsjellë preferohet kur të keni akses në sistemet e korporatave (p.sh. klienti në server dhe server te klienti).
- Siguroni aty ku është e mundur qe kompjuterët apo pajisjet e korporatave për stafin gjatë punës remote;
    - Të sigurohen që këta kompjuterë apo pajisje kanë nivele të përditësuar të programeve të sigurisë dhe niveleve të sigurisë
    - Përdoruesit t'u kujtohet rregullisht dhe periodikisht që të kontrollojnë nivelet e patch'eve.
    - Këshillohet gjithashtu që të ketë një skemë zëvendësimi për pajisjet që nuk funksionojnë.
- Në rast se aplikoni BYOD (Sillni pajisjen tuaj) siç janë laptopët personal ose pajisjet mobile duhet të vërtetohen nga pikëpamja e sigurisë duke përdorur platformat NAC, NAP. (psh. kontrolli i patch, kontrolli i konfigurimit, kontrolli AV etj.).
- Sigurohuni që janë krijuar burime të përshtatshme dhe të bollshme të TIK për të mbështetur stafin në rast të çështjeve apo problemeve teknike gjatë punës nga shtëpia;

    - Siguroni informacione specifike, p.sh. për pikat e kontaktit, për stafin.
- Mundësoni dhe rishikoni politikat dhe procedurat për t'iu përgjigjur incidenteve të sigurisë dhe shkeljeve të të dhënave personale dhe se stafi është informuar siç duhet për to.
- Sigurohuni që çdo përpunim i të dhënave të personelit nga punëdhënësi në kontekstin e punës nga shtëpia (p.sh. koha e mbajtjes dhe aksesit te tyre) është në përputhje me kornizën ligjore të Republikës së Shqipërisë dhe të BE-së për mbrojtjen e të dhënave personale (GDPR).

Rekomandime për stafin

- Përdorni kompjuter të kompanisë (në vend të atyre personal) kur është e mundur - përveç nëse BYOD është vërtetuar sipas pikës përkatëse nën Seksionin 1 më lart. Sa të jetë e mundur, mos përzieni aktivitetet e punës dhe kohës së lirë në të njëjtën pajisje dhe tregohuni veçanërisht të kujdesshëm me ndonjë e-mail që i referon virusit te koronës.
- Lidhu në internet përmes rrjeteve të sigurta; shmangni rrjetet e hapura / free. Shumica e sistemeve wifi në shtëpi këto ditë janë të siguruara, por disa instalime më të vjetra mund të mos jenë.
- Me një lidhje të pasigurt, njerëzit në afërsi (psh: në të njëjtën wireless)mund të shikojnë trafikun tuaj (më shumë njerëz teknikë mund të jenë në gjendje të rrëmbejnë apo përgjojnë lidhjen). Siç u përmend më sipër, rreziku nuk është aq më i lartë se sa kur përdorni 'rrjetet e hapura' publike, përveç faktit se njerëzit me sa duket do të jenë në të njëjtin vend për një kohë të gjatë. Zgjidhja është të aktivizoni zgjidhjet e enkriptimit nëse nuk është bërë tashmë dhe / ose të adoptoni implementimet e fundit. Vini re se ky rrezik është disi i lehtësuar duke përdorur një lidhje të sigurt me zyrën.
- Shmangni shkëmbimin e informacionit sensitiv të kompanive (p.sh. përmes e-mailit) përmes lidhjeve ndoshta të pasigurta.
- Përdorni burimet e institucionit siç është Intranet sa më shumë të jetë e mundur, për të shkëmbyer skedarë pune. Nga njëra anë, kjo siguron që skedarët e punës janë të përditësuar dhe në të njëjtën kohë, shmanget shpërndarja e informacionit sensitiv në pajisjet lokale.
- Jini veçanërisht të kujdesshëm me çdo e-mail që i referohet virusit të koronës, pasi këto mund të jenë përpjekje për phishing ose mashtrime. Në rast dyshimi në lidhje me legjitimitetin e një e-maili, kontaktoni personelin e sigurisë së institucionit.
- Të dhënat e ruajtura lokalisht, p.sh. disqet lokale, duhet të kodohen apo enkriptohen (kjo do të mbrojë kundër vjedhjes / humbjes së pajisjes).
- Programet Antivirus / Antimalware duhet të jenë të instaluara dhe të përditësuara plotësisht.
- Sistemi operativ dhe aplikacionet e përdorura, duhet të jenë të përditësuara.
- Kyçni ekranin tuaj nëse largoheni nga kompjuteri kur punoni në shtëpi, njëlloj siç do te vepronit kur punoni në zyrë.
- Mos i ndani URL-të e takimit virtual në mediat sociale ose kanalet e tjera publike. (Në këtë mënyrë palët e treta të paautorizuara mund të hynin në takime private.)

Mashtrimet phishing të lidhura me COVID-19

Është e rëndësishme të rritni vetëdijen për sigurinë dixhitale gjatë kësaj kohe pasi tashmë kemi parë një rritje të sulmeve të phishing. Hakerat janë duke shfrytëzuar situatën, kështu që shikoni me kujdes postën elektronike për mashtrime.
Në situatën aktuale, duhet të jetë dyshues për çdo e-mail që kërkon të kontrollojë ose rinovojë kredencialet tuaja, edhe nëse duket se vjen nga një burim i besueshëm. Ju lutemi provoni të verifikoni vërtetësinë e kërkesës përmes mjeteve të tjera, mos klikoni në lidhje të dyshimta ose mos hapni ndonjë bashkëngjitje (attachment) të dyshimtë.

- Bëhuni shumë dyshues për e-maile nga njerëz që nuk i njihni - veçanërisht nëse kërkojnë të lidhen me lidhje ose të hapin skedarë (nëse dyshoni telefononi personelin tuaj të sigurisë).
- E-mailet që krijojnë një imazh të urgjencës ose pasojave të rënda janë kandidatët kryesorë për phishing - në këto raste gjithmonë verifikoni përmes një kanali të jashtëm para se ti zbatoni.
- E-mailet e dërguara nga njerëz që njihni, por qe kërkojnë gjëra të pazakonta gjithashtu janë të dyshimtë - verifikoni me telefon nëse është e mundur.

Për më shume rekomandime apo këshilla të sigurisë kibernetike ju lutem referojuni burimeve zyrtare të kompanive tuaja si dhe faqes zyrtare të AKCESK ku do të publikohen periodikisht informacione dhe këshilla të sigurisë kibernetike.