PREPORUKE ZA SIGURAN RAD IZ KUĆNOG OKRUŽENJA

Kako se uslijed aktualne pandemije virusa COVID-19 sve više kompanija i organizacija odlučuje na rad zaposlenika od kuće, to otvara novi horizont mogućnosti za zlonamjerne napadače čiji je je cilj kompromitacija korporativnih i institucionalnih informacijskih sustava. Rad od kuće ne predstavlja izrazitu novinu u današnjem svijetu, međutim migracija velikog broja zaposlenika iz korporativnih okruženja koja imaju uspostavljene sustave nadzora i upravljanja informacijskom sigurnošću, u kućna okruženja s Wi-Fi vezama, predstavlja izazov za stručnjake zadužene za informacijsku sigurnost, ali i izrazitu priliku za zlonamjerne napadače.

Ovaj dokument donosi pregled rizika rada od kuće, ali i nekoliko preporuka koje na jednostavan način svode te rizike na minimalnu i prihvatljivu razinu. Treba imati u vidu da, u situacijama rada od kuće, vaše privatno okruženje postaje dio institucionalne strukture i kao karika u lancu utječe na cjelokupnu sigurnost vaše organizacije.

KIBERNETIČKI NAPADI

Zabrinutost za povezanost aktualne pandemije i kibernetičkih napada je realna. Napadači su tijekom proteklih tjedana koristili globalnu paniku oko virusa COVID-19 kako bi distribuirali od ranije poznate vrste zlonamjernog koda. Za provođenje *phishing napada* vrlo često koriste se lažne poruke elektroničke pošte koje se u svom sadržaju referenciraju na aktualnu globalnu pandemiju.

RIZICI POVEZANI S RADOM OD KUĆE

Rad od kuće otvara novi horizont napada kao posljedicu novih rizika informacijske sigurnosti koji ne postoje ili su minimalni tijekom rada iz institucionalnog okruženja.

Pristup informacijskim sustavima korištenjem potencijalno nesigurnih mreža - korisnici će tijekom rada od kuće pristupati informacijskim sustavima korištenjem kućne Wi-Fi mreže ili u gorem slučaju korištenjem javnih otvorenih Wi-Fi mreža. Ove mreže u pravilu imaju nižu razinu zaštite što otvara mogućnost kibernetičkih napada.

Korištenje privatnih računala - tijekom rada od kuće korisnici će sustavima najčešće pristupati pomoću svojih privatnih računala i mobilnih uređaja. Ti uređaji u pravilu nisu dio informacijskih sustava institucija i u pravilu imaju nižu razinu sigurnosti.

Fizička sigurnost - tijekom rada od kuće korisnici će najčešće koristiti privatna mobilna računala koja mogu biti predmet krađe ili gubitka. Gubitkom mobilnog računala kompromitiraju se i podaci koji se nalaze na njemu.

PREPORUKE ZA KRAJNJE KORISNIKE

Ove preporuke mogu značajno umanjiti rizike od potencijalne kompromitacije vašeg računala, a posljedično i čitavog informacijskog sustava institucije kojemu pristupate iz kućnog okruženja.

Odgovorno korištenje privatnog računala - suzdržite se od korištenja privatnog računala u svrhe koje mogu dodatno povećati rizik od njegove kompromitacije, kao što je pretraživanje sumnjivih internetskih stranica, preuzimanje sadržaja sa sumnjivih lokacija, on-line klađenje i slično.

Zaštita privatnih računala - ako postoje, ažurirajte antivirusne alate na svom računalu. Ako imate više računala na raspolaganju, koristite računalo s najnovijim verzijama operativnih sustava.

Ograničite pristup računalima - objasnite svojim ukućanima da je vaše računalo u ovoj situaciji poslovno računalo. Osigurajte da ostale osobe ne koriste računalo kako bi se izbjegle situacije nenamjerne izmjene ili brisanja podataka.

***Phishing* poruke** - obratite posebnu pažnju na sumnjive poruke elektroničke pošte. Ne otvarajte ih i ne preuzimajte sadržaj ako sumnjate da se radi o zlonamjernim porukama. Koristite *call back* metodu kojom prije otvaranja sumnjive poruke elektroničke pošte telefonskim putem kontaktirate pošiljatelja i provjerite je li poruka uistinu poslana s opravdanom svrhom.

Socijalni inženjering - Budite svjesni da cjelokupno okruženje rada od kuće pogoduje napadima socijalnim inženjeringom tijekom kojih vas nepoznate osobe mogu poticati na dijeljenje korisničkih podataka kao što su lozinke ili PIN-ovi.

Zapamti lozinku - izbjegavajte korištenje opcije "zapamti lozinku" dok pristupate informacijskim sustavima institucije.

Izbjegavajte javne Wi-Fi mreže - pokušajte ne koristiti javne Wi-Fi mreže dok se spajate na informacijski sustav institucije. Također, dodatno provjerite sigurnosne postavke svoje kućne mreže, provjerite lozinke i po potrebi ih promijenite. Koristite snažne lozinke, s dovoljno znakova. Osigurajte da kućni Wi-Fi koriste isključivo osobe od vašeg povjerenja.

Pristupajte isključivo sustavima nužnima za rad - tijekom rada ne prakticirajte pristup sustavima institucije koji vam nisu apsolutno nužni za rad. To se osobito odnosi na sustave koji pohranjuju ili obrađuju osjetljive vrste dokumenata. Na kraju radnog dana, dokumente na kojima ste radili pospremite na siguran USB uređaj u svrhu pričuvne pohrane (*backup).*

Preuzimanje dokumenata - ne preuzimajte službene dokumente na svoje privatno računalo ako to apsolutno nije potrebno.

Kontaktirajte - u slučaju naznake računalno-sigurnosnog incidenta ili moguće ugroze, kontaktirajte osobe odgovorne za informacijsku sigurnost u svojoj instituciji.