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 ADMINISTRATORE

Ove preporuke mogu značajno umanjiti rizike od potencijalne kompromitacije čitavog informacijskog sustava institucije koji su nastali uvođenjem rada od kuće.

Sustavno i planirano uvođenje udaljenog pristupa - potrebno je identificirati ključne računalne sustave za obavljanje redovitog poslovanja te postepeno zaposlenicima omogućavati udaljeni pristup isključivo tim sustavima s korisničke razine i isključiti pristup administracijskim sučeljima za udaljene korisnike. Potrebno je pratiti stanje na mrežnoj i sustavnoj razini prilikom postepenog uvođenja kako bi se lakše identificirali i spriječili sigurnosni rizici u infrastrukturi organizacije. U svrhu sprječavanja ispada sustava uputno je uspostaviti praćenje opterećenja sustava na pristupnoj točki.

Ažuriranje i zaštita organizacijske infrastrukture korisničkih radnih stanica - potrebno je ažurirati sve ključne poslužitelje (VPN, mail, intranet) i programsku podršku s posljednjim dostupnim sigurnosnim zakrpama. Uputno je da korisnici na svojim radnim stanicama primijene zadnje dostupne sigurnosne zakrpe i aktiviraju (instaliraju) barem osnovnu razinu antivirusne zaštite (primjerice Microsoft Defender za Windows operacijske sustave) prije udaljenog spajanja na organizacijsku infrastrukturu.

Uspostava sigurnosnih mjera za udaljeni pristup - u skladu s mogućnostima trenutne informatičke podrške potrebno je uskladiti sigurnost mehanizama prijave na sustav s pravilima dobre prakse. Primjeri dobrih sigurnosnih mjera su bilježenje dnevničkih zapisa za sva udaljena spajanja u organizaciju, uvođenje politike redovite promjene lozinki, usklađivanje složenosti korisničkih lozinki prema pravilima dobre prakse, uvođenje više-faktorske autorizacije ili dodatne zaštite za prijavu kako bi se onemogućili *brute-force* napadi na korisničke podatke.

Administracija ključnih sustava u organizaciji – ne preporuča se omogućavanje udaljene administracije ključnih sustava za rad organizacije. Uputno je administraciju takvih sustava odrađivati na lokaciji. U slučaju iznimne potrebe za udaljenom administracijom uputno je stvoriti u potpunosti nove autorizacijske podatke i zaštiti pristup svim dostupnim mehanizmima te odvojiti administracijske radnje od regularnog poslovanja udaljenih korisnika sustava.

Procjena generalne sigurnosne politike nakon uspostave udaljenog rada – povećana izloženost informacijskog sustava, zbog otvaranja pristupa korisnicima u nezaštićenoj okolini i otvaranja pristupa raznim servisima, zahtijeva provedbu procjene rizika sustava. Identificirane rizike potrebno je pravilno ukloniti i umanjiti te po potrebi provesti ponovnu segmentaciju mreže s ciljem smanjivanja izloženosti.