AGENCIJA EUROPSKE UNIJE
ZA KIBERSIGURNOST

Vodič za kibersigurnost za MSP-ove

12 KORAKA DO SIGURNOSTI VAŠEG POSLOVANJA

Kriza COVID-19 pokazala je koliko su internet i računala općenito važni za mala i srednja poduzeća (MSP). Kako bi bili poslovno uspješni tijekom pandemije, mnogi MSP-ovi morali su poduzeti mjere u pogledu kontinuiteta poslovanja, kao što su prelazak na usluge u oblaku, poboljšanje internetskih usluga, nadogradnja mrežnih mjesta i omogućavanje rada na daljinu za svoje osoblje.

U ovom se letku MSP-ovima predstavlja 12 praktičnih koraka visoke razine kojima mogu bolje osigurati svoje sustave i svoje poslovanje. Riječ je o pratećoj publikaciji uz detaljnije izvješće ENISA-e **Kibersigurnost za MSP-ove – izazovi i preporuke”**.

1 RAZVIJTE DOBRU KIBERKULTURU

DODIJELITE ODGOVORNOST UPRAVLJANJA

Dobra kibersigurnost ključni je element kontinuiranog uspjeha svakog MSP-a. Odgovornost za tu ključnu funkciju trebala bi biti dodijeljena nekome unutar organizacije tko bi trebao osigurati odgovarajuće resurse za potrebe kibersigurnosti, kao što su vrijeme osoblja, kupnja softvera, usluga i hardvera za kibersigurnost, osposobljavanje osoblja i razvoj učinkovitih pravilnika.

STEKNITE PODRŠKU ZAPOSLENIKA

Steknite podršku zaposlenika učinkovitom komunikacijom uprave o kibersigurnosti, tako da uprava otvoreno podupire inicijative za kibersigurnost, da zaposlenici dobivaju odgovarajuća osposobljavanja te da se zaposlenicima daju jasna i konkretna pravila navedena u pravilnicima o kibersigurnosti.

OBJAVLJUJTE PRAVILNIKE O KIBERSIGURNOSTI

Pravilnici o kibersigurnosti za zaposlenike trebaju sadržavati jasna i konkretna pravila o tome kakvo se ponašanje od njih očekuje kada koriste IKT okruženje, opremu i usluge poduzeća. U tim bi pravilnicima također trebale biti istaknute posljedice s kojima bi se zaposlenici mogli suočiti ako se ne pridržavaju pravilnika. Pravilnike je potrebno redovito pregledavati i ažurirati.

PROVODITE REVIZIJE KIBERSIGURNOSTI

Redovne revizije trebaju provoditi osobe s odgovarajućim znanjem, vještinama i iskustvom. Revizori bi trebali biti neovisni, bez obzira na to je li riječ o vanjskom ili internom izvođaču, te neovisni o svakodnevnim IT aktivnostima.

NE ZABORAVITE NA ZAŠTITU PODATAKA

U skladu s Općom uredbom EU-a o zaštiti podataka[1], svaki MSP koji obrađuje ili pohranjuje osobne podatke koji pripadaju rezidentima EU-a/EGP-a mora osigurati odgovarajuće sigurnosne kontrole za zaštitu tih podataka. Među ostalim, potrebno je osigurati da sve treće strane koje rade u ime MSP-a imaju uspostavljene odgovarajuće sigurnosne mjere.

1 Opća uredba o zaštiti podataka
https://ec.europa.eu/info/law/law-topic/data-protection_en

2

OMOGUĆITE POTREBNU OBUKU

Osigurajte redovita osposobljavanja za podizanje svijesti o kibersigurnosti za sve zaposlenike kako biste bili sigurni da oni mogu prepoznati različite kibersigurnosne prijetnje i da se znaju s njima nositi. Ta bi osposobljavanja trebala biti prilagođena MSP-ovima i usmjerena na situacije u stvarnom životu.

Osigurajte specijalizirano osposobljavanje iz područja kibersigurnosti za one koji su odgovorni za upravljanje kibersigurnošću unutar poduzeća kako bi se zajamčilo da imaju vještine i kompetencije potrebne za obavljanje svojeg posla.

3

OSIGURAJTE UČINKOVITO UPRAVLJANJE TREĆIM STRANAMA

Osigurajte da se svim dobavljačima, osobito onima s pristupom osjetljivim podacima i/ili sustavima, aktivno upravlja i da ispunjavaju dogovorene razine sigurnosti. Trebali bi postojati ugovori kojima se regulira način na koji dobavljači ispunjavaju te sigurnosne zahtjeve.

4

RAZVIJTE PLAN ODGOVORA NA INCIDENTE

Razvijte formalni plan odgovora na incidente koji sadržava jasne smjernice, uloge i odgovornosti dokumentirane kako bi se osiguralo da se na sve sigurnosne incidente reagira pravodobno, profesionalno i na odgovarajući način. Kako biste brzo odgovorili na sigurnosne prijetnje, istražite alate koji bi mogli nadzirati i stvarati upozorenja kada dođe do sumnjivih aktivnosti ili kršenja sigurnosti.

5 OSIGURAJTE PRISTUP SUSTAVIMA

Potičite sve da koriste pristupnu zaporku, skup od najmanje tri nasumične uobičajene riječi kombinirane u izraz koje pružaju vrlo dobru kombinaciju pamtljivosti i sigurnosti. Ako se odlučite za tipičnu lozinku:

- neka bude dugačka, s malim i velikim slovima, možda i brojevima te posebnim znakovima;
- izbjegavajte očito, kao što je „lozinka", niz slova ili brojeva kao što su „abc", brojevi kao što su „123";
- izbjegavajte upotrebu osobnih podataka koji se mogu pronaći na internetu.

Bez obzira na to upotrebljavate li pristupne zaporke ili lozinke:

- nemojte ih ponovno upotrebljavati na drugom mjestu;
- nemojte ih dijeliti sa suradnicima;
- omogućite višestruku provjeru autentičnosti;
- upotrebljavajte namjenski upravitelj lozinki.

6

ZAŠTITITE UREĐAJE

Ključni korak u programu kibersigurnosti je održavanje sigurnosti uređaja koje osoblje upotrebljava, bilo da su to njihova stolna računala, prijenosna računala, tableti ili pametni telefoni.

ODRŽAVAJTE SOFTVER ZAKRPAMA I AŽURIRANJIMA

Idealno je koristiti se centraliziranim platformama za upravljanje zakrpama. MSP-ovima se posebno poručuje:

- da redovito ažuriraju svoj softver;
- da uključe automatska ažuriranja kad god je to moguće;
- da utvrde koji softver i hardver zahtijevaju ručno ažuriranje;
- da uzmu u obzir mobilne uređaje i uređaje interneta stvari (IoT).

ANTIVIRUS

Na sve vrste uređaja treba implementirati centralno upravljano antivirusno rješenje i redovito ga ažurirati kako bi se osigurala njegova kontinuirana učinkovitost. Također, nemojte instalirati piratski softver jer može sadržavati zlonamjerni softver.

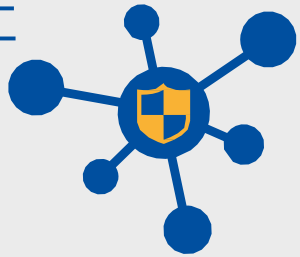
KORISTITE SE ALATIMA ZA ZAŠTITU E-POŠTE I MREŽE

Koristite se rješenjima za blokiranje neželjenih e-poruka, e-poruka s poveznicama na zlonamjerna mrežna mjesta, e-poruka koje sadržavaju zlonamjerne privitke kao što su virusi i „phishing" e-poruke.

ENKRIPCIJA/ŠIFRIRANJE

Zaštitite podatke šifriranjem. MSP-ovi bi trebali osigurati da podaci i tablice pohranjeni na mobilnim uređajima, kao što su prijenosna računala i pametni telefoni, budu šifrirani. Pobrinite se za to da podaci koji se prenose putem javnih mreža, kao što su WiFi mreže hotela ili zračnih luka, budu šifrirani, i to korištenjem virtualne privatne mreže (VPN) ili pristupanjem mrežnim mjestima putem sigurnih veza s pomoću SSL/TLS protokola. Budite sigurni da se na njihovim mrežnim mjestima primjenjuje odgovarajuća tehnologija enkripcije za zaštitu podataka klijenata dok putuju internetom.

7 ZAŠTITITE SVOJU MREŽU



IMPLEMENTIRAJTE UPRAVLJANJE MOBILNIM UREĐAJIMA

Dok omogućuju osoblju da radi na daljinu, mnogi MSP-ovi dopuštaju osoblju korištenje vlastitim prijenosnim računalima, tabletima i/ili pametnim telefonima. Time nastaje nekoliko sigurnosnih problema povezanih s osjetljivim poslovnim podacima pohranjenima na tim uređajima. Jedan od načina upravljanja tim rizikom je primjena rješenja za upravljanje mobilnim uređajima (MDM) koja MSP-ovima omogućuju:

- da kontroliraju kojim je uređajima dopušten pristup njihovim sustavima i uslugama;
- da osiguraju da uređaj ima instaliran ažurirani antivirusni softver;
- da utvrde je li uređaj šifriran;
- da potvrde jesu li na uređaj instalirane ažurirane softverske zakrpe;
- da se pobrinu da je uređaj zaštićen PIN-om i/ili lozinkom.
- da daljinski izbrišu sve MSP-ove podatke s uređaja ako vlasnik uređaja prijavi da je izgubljen ili ukraden, ili ako prestane radni odnos vlasnika uređaja kod MSP-a.

KORISTITE SE VATROZIDIMA

Vatrozidi upravljaju prometom koji ulazi u mrežu i iz nje izlazi te su jedan od najvažnijih alat u zaštiti sustava MSP-ova. Vatrozidi bi se trebali postaviti kako bi zaštitili sve najvažnije sustave, vatrozid bi se posebice trebao koristiti za zaštitu mreže MSP-a od interneta.

PREGLEDAJTE RJEŠENJA ZA DALJINSKI PRISTUP

MSP-ovi bi trebali redovito pregledavati sve alate za daljinski pristup kako bi osigurali da su sigurni, posebice:

- osigurati da sav softver za daljinski pristup ima potrebne zakrpe i da je ažuriran;
- ograničiti udaljeni pristup sa sumnjivih geografskih lokacija ili određenih IP adresa;
- ograničiti daljinski pristup osoblja samo na sustave i računala koja su im potrebna za njihov posao;
- postaviti snažne lozinke za daljinski pristup i gdje je moguće omogućiti višestruku provjeru autentičnosti;
- osigurati da su omogućeni nadzor i sustav upozoravanja kako bi se upozorilo na sumnjive napade ili neuobičajene sumnjive aktivnosti.

8 POBOLJŠAJTE FIZIČKU SIGURNOST

Gdje god se nalaze važne informacije potrebno je primijeniti odgovarajuće fizičke kontrole. Prijenosno računalo ili pametni telefon tvrtke, na primjer, ne bi trebali ostati bez nadzora na stražnjem sjedalu automobila. Svaki put kada se korisnici udalje od svojeg računala, trebali bi ga zaključati. U suprotnom, omogućite funkciju automatskog zaključavanja na svakom uređaju koji se upotrebljava u poslovne svrhe. Isto tako, osjetljive ispisane dokumente ne treba ostavljati bez nadzora, a kada se ne upotrebljavaju, treba ih sigurno pohraniti.

9 ZAŠTITITE SIGURNOS NE KOPIJE

Sigurnosne kopije treba održavati kako bi se omogućio oporavak formiranja ključa jer su one učinkovit način oporavka od katastrofa, kao što je napad ucjenjivačkog programa (engl. „ransomware"). Trebala bi se primjenjivati sljedeća pravila sigurnosnog kopiranja:

- sigurnosno kopiranje je redovito i automatizirano kad god je to moguće,
- sigurnosna kopija čuva se odvojeno od produkcijskog okruženja MSP-a,
- sigurnosne kopije su šifrirane, osobito ako se trebaju premještati s jedne lokacije na drugu,
- testira se mogućnost redovitog vraćanja podataka iz sigurnosnih kopija. U idealnom bi slučaju trebalo obaviti redoviti test potpunog vraćanja od početka do kraja.

10

ODLUČITE SE ZA OBLAK

Iako pružaju mnoge prednosti, rješenja koja se temelje na oblaku predstavljaju određene jedinstvene rizike koje bi MSP-ovi trebali razmotriti prije nego što se obrate pružatelju usluga u oblaku. ENISA je objavila „Vodič za sigurnost u oblaku za MSP-ove"[2] koji bi MSP-ovi trebali proučiti prije migracije podataka u oblak.

Pri odabiru pružatelja usluga u oblaku, MSP-ovi bi trebali osigurati da ne krši zakone ili propise pohranjivanjem podataka, posebice osobnih podataka, izvan EU-a/EGP-a. Na primjer, Općom uredbom EU-a o zaštiti podataka zahtijeva se da se osobni podaci rezidenata EU-a/EGP-a ne pohranjuju i ne prenose izvan EU-a/EGP-a osim u vrlo specifičnim uvjetima.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 OSIGURAJTE MREŽNA MJESTA

Bitno je da MSP-ovi osiguraju da su njihova mrežna mjesta konfigurirana i održavana na siguran način te da su svi osobni podaci ili financijske pojedinosti, kao što su podaci kreditnih kartica, zaštićeni na odgovarajući način. To će podrazumijevati provođenje redovitih sigurnosnih testova na mrežnim mjestima radi utvrđivanja svih potencijalnih sigurnosnih slabosti te provođenje redovitih pregleda kako bi se osiguralo da se mrežno mjesto pravilno održava i ažurira.

12 TRAŽITE I RAZMJENJUJTE INFORMACIJE

Učinkovit alat u borbi protiv kiberkriminala je razmjena informacija. Razmjena informacija u vezi s kiberkriminalom ključna je za MSP-ove kako bi bolje razumjeli rizike s kojima se suočavaju. Tvrtke koje od svojih kolega saznaju o problemima u području kibersigurnosti i o tome kako su oni te probleme prevladali, vjerojatnije će poduzeti korake za osiguravanje svojih sustava, nego da o sličnim pojedinostima saznaju iz industrijskih izvješća ili iz anketa o kibersigurnosti.

AGENCIJA EUROPSKE UNIJE ZA KIBERSIGURNOST

O ENISA-i
Agencija Europske unije za kibersigurnost, ENISA, agencija je Unije osnovana s ciljem postizanja visoke zajedničke razine kibersigurnosti u cijeloj Europi. Agencija Europske unije za kibersigurnost osnovana je 2004. na temelju Akta o kibersigurnosti EU-a i odonda pridonosi kiberpolitici EU-a, poboljšava pouzdanost proizvoda, usluga i postupaka IKT-a s pomoću programa kibersigurnosne certifikacije, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi na kiberizazove koji je očekuju u budućnosti. Agencija, zajedno sa svojim ključnim dionicima, pridonosi razmjeni znanja, izgradnji kapaciteta i informiranju kako bi se ojačalo povjerenje u povezano gospodarstvo, povećala otpornost infrastrukture Unije te kako bi se, u konačnici, sačuvala sigurnost europskog društva i građana. Više informacija dostupno je na: www.enisa.europa.eu.

ENISA
Agencija Europske unije za kibersigurnost

Ured u Ateni
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Atika, Grčka

Ured u Heraklionu
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Grčka

enisa.europa.eu