enisa

AGENCIJA EVROPSKE UNIJE ZA KIBERNETSKO VARNOST

Vodnik o kibernetski varnosti za MSP

12 KORAKOV DO VARNEGA POSLOVANJA

Med krizo zaradi covida-19 se je pokazalo, kako pomembni so internet in računalniki na splošno za MSP. Da so lahko med pandemijo uspešno poslovala, so morala številna MSP sprejeti ukrepe za neprekinjeno poslovanje, kot so prehod na storitve v oblaku, izboljšanje svojih internetnih storitev, nadgradnja svojih spletnih mest in omogočanje dela na daljavo svojim zaposlenim.

Ta brošura vključuje 12 praktičnih ukrepov na visoki ravni, s katerimi lahko MSP bolje zavarujejo svoje sisteme in poslovanje. Je spremljevalna publikacija podrobnejšega poročila agencije ENISA o izzivih in priporočilih v zvezi s kibernetsko varnostjo za MSP z naslovom **„Cybersecurity for SMEs – Challenges and Recommendations“**.

1 VZPOSTAVITE DOBRO KULTURO KIBERNETSKE VARNOSTI

DODELITE ODGOVORNOST ZA UPRAVLJANJE

Dobra kibernetska varnost je ključni element za trajni uspeh vseh MSP. Odgovornost za to kritično funkcijo bi bilo treba dodeliti osebi v organizaciji, ki bi morala zagotoviti ustrezne vire, kot so rapoložljivost zaposlenih, nakup programske opreme, storitev in strojne opreme za kibernetsko varnost, usposabljanje zaposlenih in vzpostavitev učinkovitih politik za kibernetsko varnost.

PRIDOBITE PODPORO PRI ZAPOSLENIH

Pridobite podporo pri zaposlenih z učinkovitim obveščanjem o kibernetski varnosti s strani vodstva, upravljanjem, ki odprto podpira pobude za kibernetsko varnost, ustreznimi usposabljanji ter zagotavljanjem jasnih in podrobnih pravil za zaposlene, opredeljenih v politikah kibernetske varnosti.

OBJAVITE POLITIKE KIBERNETSKE VARNOSTI

V politikah kibernetske varnosti bi bilo treba določiti jasna in podrobna pravila za zaposlene o tem, kako naj bi ravnali pri uporabi okolja, opreme in storitev IKT podjetja. V teh politikah bi morale biti jasno poudarjene tudi posledice za zaposlene, če ne bi upoštevali teh politik. Politike je treba redno pregledovati in posodabljati.

IZVAJAJTE REVIZIJE NA PODROČJU KIBRNETSKE VARNOSTI

Redne revizije bi morale izvajati osebe z ustreznimi znanji, spretnostmi in izkušnjami. Revizorji bi morali biti neodvisni, ne glede na to, ali so zunanji ali notranji izvajalci MSP, in neodvisni od vsakodnevnega delovanja informacijske tehnologije.

NE POZABITE NA VARSTVO PODATKOV

V skladu s Splošno uredbo EU o varstvu podatkov[1] morajo vsa MSP, ki obdelujejo ali shranjujejo osebne podatke rezidentov EU/EGP, zagotoviti ustrezen varnostni nadzor za zaščito teh podatkov. To vključuje zagotavljanje, da imajo vse tretje osebe, ki delujejo v imenu MSP, vzpostavljene ustrezne varnostne ukrepe.

1 Splošna uredba o varstvu podatkov https://ec.europa.eu/info/law/law-topic/data-protection_en

2

ZAGOTOVITE USTREZNO USPOSABLJANJE

Zagotovite redna usposabljanja za ozaveščanje o kibernetski varnosti za vse zaposlene, da bodo lahko prepoznali različne grožnje za kibernetsko varnost in se z njimi spoprijeli. Ta usposabljanja bi morala biti prilagojena posameznemu MSP in osredotočena na dejanske razmere.

Zagotovite specializirano usposabljanje na področju kibernetske varnosti za tiste, ki so odgovorni za upravljanje kibernetske varnosti v podjetju, da bodo imeli znanja in spretnosti ter kompetence, potrebne za opravljanje svojega dela.

3

ZAGOTOVITE UČINKOVITO UPRAVLJANJE TRETJIH OSEB

Zagotovite, da se vsi izvajalci, zlasti tisti, ki imajo dostop do občutljivih podatkov in/ali sistemov, dejavno upravljajo in dosegajo dogovorjene ravni varnosti. Sprejeti bi bilo treba pogodbene dogovore, ki bi urejali načine izpolnjevanja teh varnostnih zahtev s strani izvajalcev.

4

PRIPRAVITE NAČRT ODZIVANJA NA INCIDENTE

Pripravite uradni načrt odzivanja na incidente, ki bo vključeval jasne in dokumentirane smernice, vloge in odgovornosti, da se zagotovi pravočasen, profesionalen in ustrezen odziv na vse varnostne incidente. Za hiter odziv na varnostne grožnje preučite, katera orodja bi lahko uporabili za spremljanje in ustvarjanje opozoril v primeru sumljivih dejavnosti ali kršitev varnosti.

5 ZAGOTOVITE VAREN DOSTOP DO SISTEMOV

Spodbujajte vse, naj uporabljajo geselske fraze, ki so sestavljene iz niza najmanj treh naključnih pogostih besed, združenih v frazo, ki zagotavlja zelo dobro kombinacijo zapomljivosti in varnosti. Če se odločite za običajno geslo:

- naj bo to dolgo, vsebuje tako male kot velike črke, po možnosti pa naj vsebuje tudi številke in posebne znake.
- Izogibajte se očitnim besedam, kot so „geslo“, ter zaporedjem črk ali številk, kot so „abc“ ali „123“.
- Ne uporabljajte za geslo osebnih podatkov, ki jih je mogoče najti na spletu.

Ne glede na to, ali uporabljate geselske fraze ali gesla,

- jih ne uporabljajte nikjer drugje;
- jih ne delite s sodelavci;
- omogočite večkratno preverjanje pristnosti;
- uporabljajte namenskega upravitelja gesel.

6

ZAVARUJTE NAPRAVE

Zagotavljanje varnosti naprav zaposlenih, npr. njihovih namiznih, prenosnih in tabličnih računalnikov ali pametnih telefonov, je ključni korak v programu kibernetske varnosti.

POSKRBITE, DA JE PROGRAMSKA OPREMA BREZHIBNA IN POSODOBLJENA

Če je mogoče, uporabite centralizirano platformo za upravljanje popravkov. Zelo priporočljivo je, da MSP:

- redno posodabljajo vso svojo programsko opremo;
- vklopijo samodejne posodobitve, kadar je to mogoče;
- opredelijo programsko in strojno opremo, ki zahteva ročne posodobitve;
- upoštevajo tudi mobilne naprave in naprave interneta stvari.

UPORABLJAJTE PROTIVIRUSNE PROGRAME

Za vse vrste naprav bi bilo treba uvesti centralno upravljano protivirusno rešitev in jo redno posodabljati, da se zagotovi njena stalna učinkovitost. Prav tako ne nameščajte piratske programske opreme, saj lahko vsebuje zlonamerno programsko opremo.

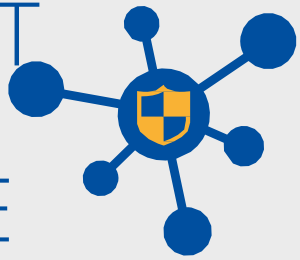
UPORABLJAJTE ORODJA ZA ZAŠČITO E-POŠTE IN SPLETA

Uporabljajte rešitve za blokiranje neželene e-pošte, e-pošte, ki vsebuje povezave do zlonamernih spletnih mest, e-pošte, ki vsebuje zlonamerne priponke, kot so virusi, in lažna e-poštna sporočila.

ŠIFRIRANJE

Podatke zaščitite tako, da jih šifrirate. MSP bi morala zagotoviti šifriranje podatkov, shranjenih na mobilnih napravah, kot so prenosni računalniki, pametni telefoni in tablice. Zagotovite, da so podatki, ki se prenašajo prek javnih omrežij, kot so hotelska ali letališka omrežja Wi-Fi, šifrirani, in sicer bodisi z uporabo virtualnega zasebnega omrežja (VPN) bodisi z dostopom do spletnih mest prek varnih povezav z uporabo protokola SSL/TLS. Zagotovite, da njihova spletna mesta uporabljajo ustrezno tehnologijo šifriranja za zaščito podatkov strank, ko potujejo po internetu.

7 ZAVARUJTE SVOJE OMREŽJE



UPORABLJAJTE REŠITVE ZA UPRAVLJANJE MOBILNIH NAPRAV

Pri omogočanju dela na daljavo številna MSP zaposlenim omogočajo uporabo lastnih prenosnih računalnikov, tabličnih računalnikov in/ali pametnih telefonov. To sproža številne varnostne pomisleke glede občutljivih poslovnih podatkov, shranjenih na teh napravah. Eden od načinov za obvladovanje tega tveganja je uporaba rešitve za upravljanje mobilnih naprav (MDM), ki MSP omogoča, da:

- nadzorujejo, katere naprave lahko dostopajo do njihovih sistemov in storitev;
- zagotovijo posodobljeno protivirusno programsko opremo v napravi;
- ugotovijo, ali je naprava šifrirana;
- ugotovijo, ali ima naprava nameščene posodobljene programske popravke;
- zagotovijo, da je naprava zaščitena s kodo PIN in/ali geslom;
- na daljavo izbrišejo vse podatke o MSP, če lastnik prijavi, da je naprava izgubljena ali ukradena, ali če se prekine delovno razmerje med lastnikom naprave in MSP.

VZPOSTAVITE POŽARNE ZIDOVE

Požarni zidovi upravljajo promet, ki vstopa v omrežje in izstopa iz njega, ter so ključno orodje za zaščito sistemov MSP. Požarne zidove bi bilo treba vzpostaviti za zaščito vseh kritičnih sistemov, zlasti pa bi moralo biti omrežje MSP zaščiteno s požarnim zidom pred internetom.

PREUČITE REŠITVE ZA ODDALJENI DOSTOP

MSP bi morala redno pregledovati vsa orodja za oddaljeni dostop, da bi zagotovila njihovo varnost, pri čemer je zlasti pomembno, da:

- zagotovijo, da je vsa programska oprema za oddaljeni dostop brezhibna in posodobljena;
- omejijo oddaljeni dostop iz sumljivih geografskih lokacij ali določenih naslovov IP;
- omejijo oddaljeni dostop zaposlenih, tako da lahko dostopajo samo do sistemov in računalnikov, ki jih potrebujejo za svoje delo;
- vzpostavijo močna gesla za oddaljeni dostop in, kadar je mogoče, omogočijo večkratno avtentikacijo;
- zagotovijo spremljanje in opozarjanje na sume napadov ali neobičajne sumljive dejavnosti.

8 POVEČAJTE FIZIČNO VARNOST

Povsod, kjer se nahajajo pomembne informacije, je treba uvesti ustrezen fizični nadzor. Prenosni računalnik podjetja ali pametni telefon na primer ne sme ostati brez nadzora na zadnjem sedežu avtomobila. Ko uporabnik odide od računalnika, ga mora vedno zakleniti. V nasprotnem primeru omogočite funkcijo samodejnega zaklepanja na vseh napravah, ki se uporabljajo za poslovne namene. Občutljivi tiskani dokumenti se prav tako ne bi smeli puščati brez nadzora in bi morali biti varno shranjeni, kadar se ne uporabljajo.

9 ZAGOTOVITE VARNOSTNE KOPIJE

Da bi omogočili obnovitev ključne sestave, bi bilo treba hraniti varnostne kopije, ki so učinkovit način za vnovično vzpostavitev po katastrofi, kot je napad z izsiljevalsko programsko opremo. Veljati bi morala naslednja pravila za varnostno kopiranje:

- varnostno kopiranje se izvaja redno in samodejno, kadar je to mogoče;
- varnostno kopiranje se izvaja ločeno od proizvodnega okolja MSP;
- varnostne kopije so šifrirane, zlasti, če se bodo prenašale z ene lokacije na drugo;
- preskusi se sposobnost rednega obnavljanja podatkov iz varnostnih kopij. V idealnem primeru bi bilo treba redno opravljati preskus popolne obnovitve od začetka do konca.

10

UPORABLJAJTE OBLAK

Rešitve, ki temeljijo na oblaku, sicer ponujajo številne prednosti, vendar predstavljajo nekaj edinstvenih tveganj, ki bi jih morala MSP upoštevati, preden začnejo sodelovati s ponudnikom storitev v oblaku. Agencija ENISA je objavila vodnik o varnosti v oblaku za MSP z naslovom „Cloud Security Guide for SMEs“[2], ki bi ga morala MSP upoštevati pri prehodu v oblak.

MSP bi morala pri izbiri ponudnika storitev v oblaku zagotoviti, da s shranjevanjem podatkov, zlasti osebnih podatkov, zunaj EU/EGP ne kršijo zakonov ali predpisov. Splošna uredba o varstvu podatkov na primer zahteva, da se osebni podatki rezidentov v EU/EGP ne shranjujejo ali prenašajo zunaj EU/EGP, razen pod zelo posebnimi pogoji.

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

11 ZAVARUJTE SPLETNA MESTA

Bistveno je, da MSP zagotovijo, da so njihova spletna mesta konfigurirana in vzdrževana na varen način ter da so vsi osebni ali finančni podatki, kot so podatki o kreditnih karticah, ustrezno zaščiteni. To vključuje izvajanje rednih varnostnih preskusov na spletnih mestih za ugotavljanje morebitnih varnostnih pomanjkljivosti in izvajanje rednih pregledov za zagotovitev, da se spletno mesto ustrezno vzdržuje in posodablja.

12 POIŠČITE IN IZMENJUJTE INFORMACIJE

Učinkovito orodje v boju proti kibernetski kriminaliteti je izmenjava informacij. Izmenjava informacij v zvezi s kibernetsko kriminaliteto je ključna za MSP, da bolje razumejo tveganja, s katerimi se soočajo. Podjetja, ki se seznanijo z izzivi na področju kibernetske varnosti in načini, kako so bili ti izzivi premagani, pogosteje kot druga primerljiva podjetja sprejmejo ukrepe za zaščito svojih sistemov, kot če bi podobne podatke pridobila iz poročil industrije ali raziskav na področju kibernetske varnosti.

AGENCIJA EVROPSKE UNIJE ZA KIBERNETSKO VARNOST

O AGENCIJI ENISA

Agencija Evropske unije za kibernetsko varnost, ENISA, je agencija Unije, katere cilj je dosegati visoko skupno raven kibernetske varnosti po vsej Evropi. Ustanovljena je bila leta 2004, njene pristojnosti pa so bile okrepljene z uredbo EU o kibernetski varnosti. Prispeva h kibernetski politiki EU, povečuje zaupanje v produkte, storitve in procese IKT s certifikacijskimi shemami za kibernetsko varnost, sodeluje z državami članicami in organi EU ter pomaga Evropi, da bo pripravljena na kibernetske izzive prihodnosti. Z izmenjavo znanja, krepitvijo zmogljivosti in ozaveščanjem sodeluje s svojimi ključnimi deležniki, da bi okrepila zaupanje v povezano gospodarstvo, povečala odpornost infrastrukture Unije ter navsezadnje zagotovila digitalno varnost evropske družbe in državljanov. Za več informacij obiščite spletno mesto www.enisa.europa.eu.

ENISA
Agencija Evropske unije za kibernetsko varnost

Pisarna v Atenah
Ethnikis Antistaseos 72
in Agamemnonos 14,
Chalandri 15231, Attiki,
Grčija

Pisarna v Heraklionu
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Grčija

enisa.europa.eu