Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Vodič za kibernetičku sigurnost za mala poduzeća

Složenost sadržaja
JEDNOSTAVAN ● ○ ○

cyber.gov.au

Uvod

Za malo poduzeće, čak i manji incident u vezi s kibernetičkom sigurnošću može imati razorne posljedice.
Ovaj vodič uključuje osnovne sigurnosne mjere koje će vam pomoći u zaštiti poslovanja od uobičajenih prijetnji kibernetičkoj sigurnosti. Za početak preporučujemo sljedeće tri mjere:

- **Uključite autentifikaciju s više faktora**
- **Ažurirajte softver**
- **Napravite sigurnosnu kopiju svojih podataka**

Ovaj vodič može uključivati mjere koje nisu relevantne za vašu poslovnu djelatnost, ili vaša poslovna djelatnost može iziskivati složenije mjere. Nakon dovršetka ovog vodiča, preporučujemo malim poduzećima da implementiraju prvu razinu zrelosti Essential Eight.
Ako imate pitanja o ovim savjetima ili kibernetičkoj sigurnosti u širem smislu, preporučujemo da razgovarate s IT stručnjakom ili pouzdanim savjetnikom.

Posjetite cyber.gov.au kako biste pročitali naš cjeloviti vodič, uključujući i savjete o tome kako trebate primijeniti svaku od predloženih mjera.

Sadržaj

Prijetnje malim poduzećima

Lažne poruke

Prijevare su uobičajen način na koji kibernetički kriminalci napadaju mala poduzeća. Njihov cilj je prevarom navesti vas ili vaše osoblje na:

- slanje novca ili poklon kartica
- klikanje na zlonamjerne poveznice ili privitke
- odavanje osjetljivih informacija, kao što su lozinke.

Kibernetički kriminalci mogu pokušati prevariti vaše poduzeće putem e-pošte, tekstualnih poruka, telefonskih poziva i društvenih medija. Često će se pretvarati da su osoba ili organizacija kojoj vjerujete.

Napadi krađe identiteta (phishing attacks)

posebno zabrinjavajući **napadi čiji je cilj krađa identiteta**. Ove prijevare često sadrže poveznicu na lažnu web stranicu gdje vas se potiče da se prijavite na račun ili unesete povjerljive podatke.

Napadi sa ciljem krađe identiteta obično ugrožavaju lozinke vašeg računa. Kibernetički kriminalci se često koriste ovom metodom za "preuzimanje" računa malih poduzeća na društvenim mrežama i traženje otkupnine od njih.

Načini ublažavanja

Ako je poruka od poznatog entiteta, ali vam se učini sumnjivom, budite oprezni. Zasebno kontaktirajte osobu ili tvrtku da provjerite je li poruka legitimna. Upotrijebite kontakt podatke koje ste našli u legitimnom izvoru, na primjer službenoj web stranici tvrtke, a ne one koji se nalaze u sumnjivoj poruci.

Saznajte više o prepoznavanju prijevara i krađe identiteta pomoću sljedećih resursa:

- Prepoznajte i prijavite prijevare
- Naučite kako ćete uočiti prijevare usmjerene na krađu identiteta
- Otkrivanje društveno projektiranih poruka.

Studija slučaja:

Zaposlenica u kurirskoj tvrtki primila je e-poruku od jednog od rukovoditelja tvrtke u kojoj od nje traži da kupi 6 x $500 unaprtijed plaćenih MasterCard kreditnih kartica. Rukovoditelj joj je rekao da to drži u tajnosti, jer će kartice biti poklon bonovi za članove osoblja. Nakon kupnje, zaposlenici je rečeno da fotografira obje strane kartica i pošalje ih izvršnom direktoru kao dokaz kupnje.

Prema uputama, zaposlenica je otišla u poštu i svojom osobnom kreditnom karticom je kupila darovne kartice. Odgovorila je na rukovoditeljov e-mail i poslala fotografije darovnih kartica kao dokaz.

Nakon povratka iz pošte, zaposlenica je dala kupljene kartice izvršnom direktoru - koji ništa nije znao o njima. Nakon pregleda, **ustanovili su da su sve e-poruke o darovnim karticama stigle sa nasumične adrese e-pošte, a ne sa legitimnog računa e-pošte rukovoditelja. To je bila prijevara.**

Napadi e-poštom

Povrh prijevara, kao što je krađa identiteta, čest napad e-poštom na mala poduzeća je i **kompromitacija poslovne e-pošte** (BEC). Kriminalci se mogu lažno predstaviti kao poslovni predstavnici, preko kompromitiranih računa e-pošte ili na neki drugi način – kao što je korištenje naziva domene koji izgleda slično stvarnoj poslovnoj djelatnosti. Osim krađe podataka, cilj ovih napada je obično prijevara žrtvi kojom se navode da pošalju sredstva na bankovni račun prevaranta.

Načini ublažavanja

Najbolja obrana od napada putem e-pošte je obuka i podizanje svijesti zaposlenika. Pobrinite se da vaše osoblje zna da uvijek treba biti na oprezu s e-poštom ako primi nešto od sljedećeg:

- zahtjeve za plaćanje, posebno ako se tvrdi da su hitni ili da kasne
- promjenu bankovnih podataka
- adresu e-pošte koja ne izgleda sasvim ispravno, kao što je naziv domene koji ne odgovara u potpunosti nazivu tvrtke dobavljača.

Iako ti napadi mogu biti tragični, mjere za ublažavanje su jednostavne i ne koštaju gotovo ništa. **Kada osoblje primi ovakvu e-poštu, najučinkovitija mjera za ublažavanje je da nazove pošiljatelja i potvrdi da je zahtjev legitiman.** Nemojte koristiti kontakt podatke koji su vam poslani, jer bi mogli biti lažni. Uvedite službene postupke koje će osoblje primijeniti kada zaprimi zahtjeve za plaćanje ili promjenu bankovnih podataka.

Naučite kako možete zaštititi svoje poduzeće od BEC prijevara i kompromitacije e-pošte pomoću sljedećih resursa:

- Kompromitiranje poslovne e-pošte
- Zaštitite svoje poslovanje od prijevare putem e-pošte i kompromitiranja
- Što trebate učiniti ako je vaše poduzeće bilo meta prijevare putem e-pošte ili kompromitacije.

Studija slučaja:

Mala građevinska tvrtka je primila e-poruku od svog dobavljača u kojoj navodni dobavljač javlja da je promijenio banku. Dobavljač je dao novi broj bankovnog računa na koji se trebaju vršiti plaćanja njegovih faktura. Budući da se e-pošta činila legitimnom, **građevinska tvrtka nije nazvala dobavljača da potvrdi promjenu podataka njegovog bankovnog računa.**

Tvrtka je platila fakturu dobavljača koja je iznosila više od $70.000. Sljedećeg dana je drugi zaposlenik greškom ponovno platio istu fakturu, dakle ponovno više od $70.000. Ukupno je na novi bankovni račun navodnog dobavljača uplaćeno preko $150.000.

Kada je tvrtka nazvala svog dobavljača i zamolila ga da vrati duplu uplatu, dobavljač je rekao da ti bankovni podaci nisu točni. Odmah je pokrenuta istraga i dobavljač je otkrio da je jedan od njegovih računa e-pošte bio hakiran i da je slao lažne podatke o bankovnom računu. **Sredstva nisu vraćena.**

Zlonamjerni softver

Zlonamjerni softver (malware) je opći pojam za zlonamjerni softver osmišljen da uzrokuje štetu, na primjer ransomware, virusi, spyware i trojanci. Zlonamjerni softver (malware) može:

- ukrasti ili zaključati datoteke na vašem uređaju
- ukrasti brojeve vaših bankovnih računa ili kreditnih kartica
- ukrasti vaša korisnička imena i lozinke
- preuzeti kontrolu nad vašim računalom ili špijunirati ga.

Zlonamjerni softver može spriječiti ispravan rad vašeg uređaja, izbrisati ili oštetiti vaše datoteke ili omogućiti drugima pristup vašim osobnim ili poslovnim podacima. Ako je vaš uređaj zaražen zlonamjernim softverom, mogli biste biti izloženi i drugim napadima. Zlonamjerni softver se također može proširiti i na druge uređaje na vašoj mreži.

Vaš uređaj može biti zaražen zlonamjernim softverom na više načina, uključujući:

- posjećivanjem web stranica koje su zaražene zlonamjernim softverom
- preuzimanjem zaraženih datoteka ili softvera sa interneta
- otvaranjem zaraženih privitaka elektroničke pošte.

Ransomware (ucjenjivački softver)

Ransomware je česta i opasna vrsta zlonamjernog softvera (malware). Funkcionira tako što zaključava ili šifrira vaše datoteke, tako da im više ne možete pristupiti. Za vraćanje pristupa datotekama potrebna je otkupnina, obično u obliku kriptovalute. Kibernetički kriminalci također mogu prijetiti da će objaviti ili prodati podatke na mreži ako se ne plati otkupnina.

Načini ublažavanja

Iako vam antivirusni ili sigurnosni softver može pomoći u zaštiti od zlonamjernog softvera, nijedan softver nije 100% učinkovit. Osoblje mora paziti na e-poštu, web stranice i preuzimanje datoteka, te redovito ažurirati svoje uređaje kako bi uvijek bili sigurni.

Za više informacija o zaštiti vašeg poduzeća od ransomwarea, pogledajte sljedeće resurse:

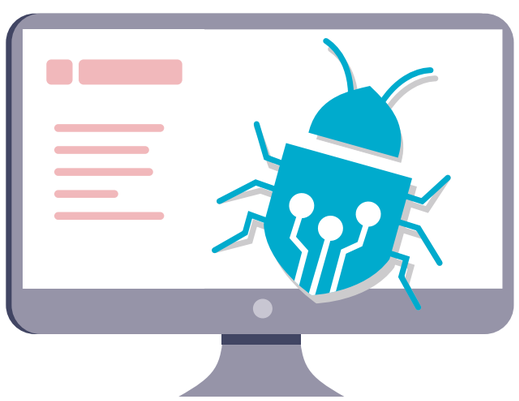
- Ransomware
- Zaštitite se od napada ucjenjivačkog (ransomware) softvera
- Što trebate činiti ako od vas traže otkupninu.

Studija slučaja:

Zaposlenici trgovine autodijelova su jednog jutra došli na posao i nisu mogli pokrenuti svoje poslužiteljsko računalo. Kada je njihov IT pružatelj usluga dobio pristup poslužitelju, pronašli su otvoren prozor u kojem je pisalo da su svi računalni podaci šifrirani. U poruci se od njih zahtijevalo da plate otkupninu u bitkoinima za otključavanje datoteka.

U računalo je bio priključen rezervni pogon, koji je također bio šifriran. Pokušali su spojiti više pogona za sigurnosnu kopiju, ali datoteke su bile automatski šifrirane u roku od nekoliko sekundi. **Nisu uspjeli ukloniti ransomware prije nego što su pokušali povratiti svoje podatke i izgubili su sve sigurnosne kopije datoteka koje su imali.**

Jedina preostala opcija je bila vratiti server na tvorničke postavke i početi iznova s novim sustavom. Njihovo poslovanje je izgubilo podatke od više godina i moralo je krenuti iznova.



Zaštitite svoje račune

Uključite višefaktorsku provjeru autentičnosti

Višefaktorska provjera autentičnosti (Multi-factor authentication) (MFA) otežava kibernetičkim kriminalcima pristup vašim računima.

MFA vašem računu dodaje još jedan sloj sigurnosti. To je jedan od najučinkovitijih načina za zaštitu računa kojim se sprječava neovlašteni pristup, pa biste ga trebali koristiti gdje god je to moguće. Svatko tko se prijavljuje na vaš račun će morati unijeti još nešto osim vašeg korisničkog imena i lozinke. To može biti jedinstveni kod iz tekst poruke ili aplikacije za provjeru autentičnosti. Za više informacija, pročitajte naše savjete o MFA na **cyber.gov.au/mfa**.

✓ **Uključite MFA gdje god je to moguće, počevši od vaših najvažnijih računa.**

Primjenjujte kontrole pristupa

Ograničavanje korisničkog pristupa može ograničiti štetu uzrokovanu incidentom koji je ugrozio kibernetičku sigurnost.

Kontrola pristupa je jedan od načina na koji se ograničava pristup određenim datotekama i sustavima. Osoblju obično nije potreban potpuni pristup svim podacima, računima i sustavima u poduzeću. Treba im se dopustiti samo pristup onome što im je potrebno za obavljanje njihovih dužnosti.

Ograničavanje pristupa će pomoći u ograničavanju štete koja nastane uslijed kibernetičkog sigurnosnog incidenta. Na primjer, ako je računalo člana osoblja zaraženo ransomwareom, uz pravilnu kontrolu pristupa bi to moglo utjecati samo na mali broj datoteka, a ne na cjelokupno poduzeće.

✓ **Pobrinite se za to da svaki korisnik može pristupiti samo onome što mu je potrebno za njegovu ulogu.**

Koristite jake lozinke ili zaporke

Zaštitite svoje račune od kibernetičkih kriminalaca sigurnom lozinkom ili zaporkom.

Mnoga mala poduzeća se suočavaju s kibernetičkim napadima zbog slabih lozinki. Na primjer, ponovna upotreba iste lozinke na više računa. Za stvaranje jakih lozinki možete koristiti i upravitelje lozinki i zaporki.

Upravitelj lozinki djeluje poput virtualnog sefa za vaše lozinke. Možete ga koristiti za stvaranje i pohranjivanje jakih, **jedinstvenih** lozinki za svaki od vaših računa. Tako, ako imate veći broj računa, ne morate pamtiti jedinstvenu lozinku za svaki od njih. Ne morate pamtiti lozinke ili račune kojima pripadaju, jer je sve pohranjeno u upravitelju lozinki.

Za račune na koje se redovito prijavljujete ili koje inače ne želite pohraniti u upravitelju lozinki, razmislite o korištenju zaporke kao svoje lozinke. Zaporke su kombinacija nasumičnih riječi, na primjer "kristalni perec od luka i gline". One su korisne kada želite sigurnu lozinku koju je lako zapamtiti. Upotrijebite nasumičnu kombinaciju četiri ili više riječi i neka bude jedinstvena –**nemojte ponovno upotrebljavati tu zaporku<** na više računa. Za više informacija pročitajte naše savjete o zaporkama i upraviteljima lozinki na **cyber.gov.au/passphrases**.

✓ **Upotrijebite upravitelja lozinki za stvaranje i pohranjivanje jedinstvenih lozinki za svaki od vaših važnih računa.**

Upravljanje zajedničkim računima

Zajednički računi mogu ugroziti sigurnost i otežati praćenje zlonamjernih aktivnosti.

U malim poduzećima mogu postojati opravdani razlozi zašto osoblje mora koristiti zajedničke račune, ali to treba izbjegavati što je više moguće. Kada više zaposlenika koristi isti račun, može biti teško pratiti aktivnost do određenog zaposlenika, a još teže pratiti kibernetičke kriminalce koji provaljuju. Ako ne promijenite lozinku, zaposlenici također mogu nastaviti pristupati računima, čak i nakon što napuste poduzeće.

✓ **Ograničite korištenje zajedničkih računa i zaštitite one koji se koriste u vašem poslovanju.**

Zaštitite svoje uređaje i podatke

Ažurirajte svoj softver

Ažuriranje softvera je jedan od najboljih načina da zaštitite svoje poduzeće od kibernetičkog napada.

Ažuriranja mogu popraviti sigurnosne nedostatke u vašem operativnom sustavu i drugom softveru, tako da je kibernetičkim kriminalcima teže provaliti. Stalno se otkrivaju novi nedostaci, stoga nemojte ignorirati poruke za ažuriranje. Redovito ažuriranje softvera će smanjiti mogućnost da kibernetički kriminalci upotrijebe poznatu slabost za pokretanje zlonamjernog softvera ili hakiranje vašeg uređaja. Ako vam je potrebna pomoć, ACSC je objavio smjernice za ažuriranja.

Ako su vaši uređaji ili softver već zastarjeli, ažuriranja možda neće biti dostupna. Ako je proizvođač prestao podržavati proizvod ažuriranjima, trebali biste razmisliti o nadogradnji na noviji proizvod kako biste bili zaštićeni. Primjeri sustava koji više ne primaju velika ažuriranja su **iPhone 7** i **Microsoft Windows 7**.

Za više informacija, pročitajte naše upute o ažuriranjima na **cyber.gov.au/updates**.

✓ **Uključite automatsko ažuriranje svojih uređaja i softvera.**

Koristite sigurnosni softver

Sigurnosni softver poput zaštite od virusa i ransomwarea može pomoći u zaštiti vaših uređaja.

Upotrijebite sigurnosni softver za otkrivanje i uklanjanje zlonamjernog softvera sa vaših uređaja. Antivirusni softver se može podesiti za redovito skeniranje sumnjivih datoteka i programa. Kada se pronađe prijetnja, primit ćete upozorenje i sumnjiva datoteka će se staviti u karantenu ili ukloniti.

Mnoga mala poduzeća mogu **koristiti Windows Security** da se zaštite od virusa i zlonamjernog softvera. Program Windows Security je ugrađen u uređaje sa sustavom Windows 10 i Windows 11 i uključuje besplatnu zaštitu od virusa i prijetnji. Možete ga koristiti i za uključivanje zaštite od ransomwarea na svom uređaju.

Za alternativne proizvode i opcije, pročitajte naše savjete o antivirusnom softveru, pretraživanjem *antivirusa* na cyber.gov.au.

✓ **Postavite sigurnosni softver za redovita skeniranja vaših uređaja.**

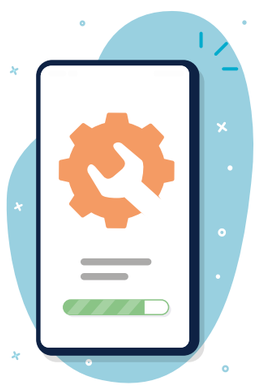
Napravite sigurnosnu kopiju svojih podataka

Redovita izrada sigurnosnih kopija vam može pomoći da povratite svoje podatke ako se izgube ili budu ugroženi.

Izrada sigurnosne kopije važnih podataka bi se trebala redovito obavljati ili se uvesti kao automatska praksa u vaše poslovanje. Bez sigurnosnih kopija koje redovno pravite bi moglo biti nemoguće povratiti podatke nakon cyber napada.

Ima raznih metoda i proizvoda koje možete koristiti za izradu sigurnosnih kopija svojih podataka. Za detaljne savjete o sigurnosnim kopijama podataka poslovanja, pročitajte naše savjete za sigurnosne kopije na **cyber.gov.au/backups**. Koja je najbolja opcija će biti različito za svako poduzeće, stoga, ako niste sigurni, razgovarajte s IT stručnjakom.

✓ **Sačinite i implementirajte plan za redovitu izradu sigurnosnih kopija vaših podataka.**



Osigurajte svoju mrežu i vanjske usluge

Zaštitite svoje poduzeće od kibernetičkih napada uklanjanjem potencijalne ranjivosti u vašoj mreži.

Uređaji i usluge u vašoj mreži mogu biti glavna meta kibernetičkih kriminalaca. Može biti komplicirano zaštititi mnoge od ovih sustava, stoga porazgovarajte o sljedećim preporukama s IT stručnjakom.

- **Zaštitite svoje poslužitelje**: Ako koristite NAS ili nekog drugog poslužitelja kod kuće ili u poduzeću, njih posebno zaštitite. Ti uređaji su česta meta kibernetičkih kriminalaca, jer se u njima često nalaze važne datoteke ili se njima obavljaju važne funkcije. Za zaštitu ovih uređaja su potrebne mnoge strategije za ublažavanje. Na primjer, važno je osigurati da se svaki poslužitelj ili NAS uređaj redovito ažurira. Administrativni računi trebaju biti zaštićeni snažnom šifrom ili autentifikacijom s više faktora.
- **Minimalizirajte vanjski otisak**: Vršite reviziju i osigurajte sve usluge izložene internetu na vašoj mreži. To može uključivati rad na daljinu, podjelu datoteka, web-poštu i usluge daljinske administracije.
- **Prebacivanje na usluge u oblaku:** Razmislite o korištenju mrežnih usluga ili usluga u oblaku koje nude ugrađenu zaštitu, umjesto da upravljate svojom vlastitom. Na primjer, koristite mrežne usluge za stvari kao što su e-pošta ili hosting web stranica umjesto da sami rukujete i osiguravate te usluge.
- **Poboljšajte sigurnost svog usmjerivača (router):** Slijedite naše upute o načinima za zaštitu usmjerivača (router), uključujući ažuriranje zadanih lozinki, uključivanje Wi-Fi mreže za goste, korisnike ili posjetitelje i korištenje najjačih protokola šifriranja. Za više informacija, potražite *router* na **cyber.gov.au**.
- **Trebate naučiti kakav je vaš kibernetički lanac opskrbe:** Suvremena poduzeća često angažiraju podugovarače za više usluga. Na primjer, koriste pružatelja usluga za održavanje njihovog IT-a. Sigurnosni problemi s ovim uslugama ili pružateljima mogu imati značajan utjecaj na vaše poslovanje. Za detaljne savjete o upravljanju rizikom u kibernetičkom lancu opskrbe pročitajte naše Upute za kibernetički lanac opskrbe na **cyber.gov.au**.

✓ **Razgovarajte s IT stručnjakom o načinima na koje možete zaštititi svoju mrežu.**

Ojačajte svoju web stranicu

Web stranice su glavna meta kibernetičkih napada.

Zaštitite svoju web stranicu od otmice pridržavajući se nekih osnovnih sigurnosnih mjera:

- osigurajte prijavu na vašu web stranicu višefaktorskom autentifikacijom ili jakom lozinkom
- redovito ažurirajte sustave za upravljanje sadržajem i dodatke vaše web stranice
- redovito pravite sigurnosne kopije vaše web stranice kako biste je mogli povratiti nakon cyber napada.

ACSC ima dodatne resurse dostupne vlasnicima web stranica. Potražite te resurse na **cyber.gov.au**:

- Strategije za vašu web stranicu koje donose brze rezultate
- Uvođenje certifikata, TLS, HTTPS i Opportunistic TLS
- Sigurnost sustava naziva domena za vlasnike domena
- Priprema za napade kojima se uskraćuju usluge i odgovor na te napade

✓ **Pročitajte resurse ACSC-a o sigurnosti web stranica.**

Resetirajte svoje uređaje prije nego što ih prodate ili bacite

Nepoznati ljudi bi mogli pristupiti podacima na vašim starim uređajima.

Ako svoje uređaje ne zbrinete na siguran način, kibernetički kriminalci mogu pristupiti podacima na njima. To može uključivati e-poštu, datoteke i druge poslovne podatke. Uklonite sve informacije sa svojih poslovnih uređaja prije nego što ih prodate, zamijenite ili bacite. Na primjer, resetiranjem na tvorničke postavke. To će vam pomoći da obrišete sve informacije i vratite uređaj na izvorne postavke.

Za savjete o ponovnom postavljanju uređaja, pročitajte naše smjernice o odlaganju uređaja na siguran način. Pretražite naslov *dispose (odlaganje)* na **cyber.gov.au**.

✓ **Prije prodaje ili odlaganja poslovnih uređaja, vratite ih na tvorničke postavke.**

Držite svoje uređaje zaključane i zaštitite ih i fizički

Ograničavanje pristupa vašim poslovnim uređajima će smanjiti prilike za zlonamjerne aktivnosti.

Ograničavanje fizičkog pristupa vašim poslovnim uređajima je jednostavan način na koji možete spriječiti krađu podataka ili druge zlonamjerne aktivnosti. Poslovni uređaji se ne bi trebali držati na mjestima na kojima im mogu pristupiti neovlašteni zaposlenici ili građani.

Primijenite sigurnosne kontrole za dodatnu zaštitu svojih poslovnih uređaja. Uređaji bi se u najmanju ruku trebali zaključavati zaporkom, PIN-om ili biometrijskim podacima. Provjerite jesu li vaši uređaji postavljeni na automatsko zaključavanje nakon kratkog razdoblja neaktivnosti.

✓ **Konfigurirajte uređaje da se automatski zaključavaju nakon kratkog vremena neaktivnosti.**

Zaštitite svoje poslovne podatke

Podaci koje posjeduje vaša tvrtka su privlačna meta za kibernetičke kriminalce.

Povrede podataka su u porastu - nemojte dopustiti da vaše poduzeće postane žrtva. Važno je razumjeti koje podatke vaše poduzeće ima i na kojim lokacijama. Kada postanete svjesni toga, pridržavajte se preporuka u ovom vodiču kako biste kibernetičkim kriminalcima onemogućili pristup vašim podacima. Neki mali poduzetnici mogu imati i dodatne obveze prema zakonu.

- **Konsolidirajte svoje poslovne podatke.** Možda imate podatke pohranjene na brojnim uređajima ili uslugama. Kada su podaci decentralizirani, povećava se broj sustava za čiju sigurnost morate brinuti i izrađivati sigurnosne kopije. Brojni sustavi također mogu stvoriti više mogućnosti za napad kibernetičkih kriminalaca. Ako je to moguće, pohranite svoje poslovne podatke na središnje mjesto koje je sigurno i za koje se redovito izrađuju sigurnosne kopije. Centraliziranje podataka može dovesti do većeg proboja ako su vaši sustavi ugroženi, zato osigurajte da to središnje mjesto bude odgovarajuće zaštićeno sigurnim konfiguracijama i ograničenim pristupom. Za savjet se obratite stručnjaku za informatičku tehnologiju ili kibernetičku sigurnost.
- **Upoznajte se sa svojim obvezama za zaštitu podataka.** Neka mala poduzeća mogu imati zakonske obveze za rukovanje osobnim podacima koje prikupljaju. Za više informacija, pročitajte vodič za mala poduzeća koji je izdao ured australskog povjerenika za informiranje, a koji je dostupan na **oaic.gov.au**. Posavjetujte se s pravnim stručnjakom ako niste sigurni.

✓ **Morate razumjeti podatke koje vaše poduzeće posjeduje i svoje odgovornosti za njihovu zaštitu.**

Pripremite svoje osoblje

Educirajte zaposlenike

Zaposlenici koji primjenjuju odgovarajuće mjere za zaštitu kibernetičke sigurnosti su vaša prva crta obrane od kibernetičkih napada.

Vaši zaposlenici bi trebali biti upoznati s kibernetičkom sigurnošću, uključujući sljedeće teme:

- uobičajene prijetnje kibernetičkoj sigurnosti, kao što su kompromitacija poslovne e-pošte i ransomware
- zaštitne mjere, uključujući jake lozinke ili šifre, MFA i ažuriranja softvera
- kako prepoznati prevare i phishing napade
- specifična pravila poslovanja (na primjer, procese za prijavu sumnjivih e-poruka ili provjeru autentičnosti faktura prije plaćanja)
- što učiniti u hitnim slučajevima.

Web stranica ACSC-a ima resurse o većini ovih tema na cyber.gov.au/learn. Možete razmisliti o drugim načinima na koje možete educirati zaposlenike, na primjer formalnim tečajem ili internim osposobljavanjem. Kako god odlučite, imajte na umu da obuka o kibernetičkoj sigurnosti nije jednokratna potreba i treba je povremeno ponavljati.

✓ **Odredite kako će se u vašem poduzeću podizati svijest o kibernetičkoj sigurnosti.**

Napravite plan za slučaj opasnosti

Postojanje plana za slučaj opasnosti bi moglo umanjiti utjecaj kibernetičkog napada na vaše poslovanje.

Prilikom reagiranja na incident koji je ugrozio kibernetičku sigurnost, svaka minuta je bitna. Ako uspostavite plan za hitne slučajeve, vaše osoblje će utrošiti manje vremena na pronalaženje rješenja, a više vremena na poduzimanje potrebnih radnji.

Razmotrite sljedeća pitanja prilikom izrade plana za slučaj opasnosti:

- Koje postupke za prijavljivanje potencijalne povrede kibernetičke sigurnosti treba primijeniti vaše osoblje?
- Kome ćete se obratiti za pomoć? Na primjer, IT stručnjacima i vašoj banci.
- Kako će se incident priopćiti vašem osoblju, dioničarima ili klijentima?
- Kako ćete upravljati uobičajenim poslovanjem, ako bilo koji kritični sustav nije povezan s internetom?

Provjerite je li vaše osoblje upoznato s planom za hitne slučajeve, uključujući sve uloge ili odgovornosti koje mogu imati. Držite tiskani primjerak plana u slučaju da vam zatreba kada sustavi ne budu povezani s internetom.

✓ **Napravite plan za hitne slučajeve za povrede kibernetičke sigurnosti.**

Budite informirani

Postanite ACSC partner kako biste primali najnovije informacije od ACSC-a.

Budite informirani o najnovijim kibernetičkim prijetnjama i ranjivostima tako što ćete postati partner ACSC-a. Ova usluga znači da će vam se svakog mjeseca slati bilteni i upozorenja kada se otkrije nova kibernetička prijetnja.

Kibernetička sigurnost je područje koje se brzo razvija. Kibernetički kriminalci aktivno iskorištavaju ranjivosti unutar nekoliko minuta nakon njihova otkrića. Informiranje o kibernetičkoj sigurnosti će pomoći vašem poduzeću da razumije prijetnje s kojima će se vjerojatno suočiti i kako se može zaštititi od njih.

✓ **Registrirajte svoje poduzeće u programu ACSC partnerstva.**

Odricanje od odgovornosti.
Materijal u ovom vodiču je općenite naravi i ne treba ga smatrati pravnim savjetom, niti se na njega treba oslanjati za pomoć u bilo kojoj konkretnoj okolnosti ili hitnoj situaciji. U svim važnim stvarima biste trebali zatražiti odgovarajući, neovisni stručni savjet u odnosu na vlastite okolnosti.

Commonwealth ne prihvaća nikakvu odgovornost za bilo kakvu štetu, gubitak ili trošak koji nastane uslijed oslanjanja na informacije u ovom vodiču.

Za više informacija ili za prijavu incidenata kibernetičke sigurnosti, kontaktirajte nas:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Ovaj broj je dostupan samo unutar Australije.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre