VODIČ ZA CYBER SIGURNOST

Za mala i srednja preduzeća

Autori

Fernala Sejmen-Banjac

Lejla Trokić

Srđan Rajčević

Sadržaj

Sadržaj....1
Partneri projekta....2
Autori....3
Uvod....4
Definicije....5
Nulta tačka: Odabir pouzdanog partnera za cyber sigurnost....6
1. Upravljanje imovinom – Inventura resursa i sistema....7
2. Klasifikacija podataka i nivoi odgovornosti....9
3. Upravljanje rizicima....10
4. Upravljanje identitetom i pristupom (Identity and Access Management - IAM)....12
5. Upravljanje uređajima i ranjivostima....14
6. Kontinuirana nadogradnja i ažuriranje....16
7. Rad na daljinu - Zaštita....17
8. Sigurnost podataka....18
9. Rezervne kopije podataka (Backup)....19
10. Logiranje i monitoring....20
11. Upravljanje incidentima....21
12. Obuka i podizanje svijesti o cyber sigurnosti....23
13. Sigurnost lanca snabdijevanja....25
Reference....26

Partneri projekta

Vodič za cyber sigurnost za mala i srednja preduzeća je nastao u saradnji sa Cranfield University UK. Projekt je podržan sredstvima Vlade Velike Britanije. Promocija projekta podržana je od strane Women4Cyber Bosna i Hercegovina.

Autori

fernala@smesecurity.ba

Fernala Sejmen- Banjac, Izvršna direktorica

Fernala Sejmen-Banjac je izvršna direktorica kompanije DISTI, sa više od 25 godina iskustva u implementaciji IT i CS rešenja. Specijalizovana za sisteme zaštite podataka, posjeduje industrijske certifikate, uključujući prestižne akreditacije u sajber sigurnosti. Kao predsjednica Women4Cyber Chapter-a za BiH, aktivno se zalaže za veću uključenost žena u sajber sigurnosti, organizujući edukacije i podižući svijest o sajber napadima.

Lider je u implementaciji sigurnosnih mreža i data centara, sa fokusom na zaštitu osjetljivih podataka. Njeni projekti obuhvataju saradnju s globalnim vendoriima, a kroz rad u javnom i privatnom sektoru izgradila je ugled stručnjaka. Godine 2023. učestvovala je u Chevening Cyber Security Fellowship programu u UK, gdje je proširila znanje o izazovima u sajber sigurnosti, analizi rizika i zaštiti malih preduzeća. Njeni napori za unapređenje IT obrazovanja uključuju rad na promjeni nastavnih planova i uključivanje stručnjaka iz prakse.

lejla@smesecurity.ba

Lejla Trokić, Stručni savjetnik za cyber sigurnosti

Lejla Trokić je stručni savjetnik za cyber sigurnost. Tokom svoje profesionalne karijere, radeći na brojnim projektima razvijala je 'secure by design' rješenja u industriji platnih i finansijskih tehnologija. Dizajnirala je PCI certificiranu serverless arhitekturu platnih procesora, implementirala osigurane sisteme i rješenja za banke i finansijske institucije.

Magistrirala je Cyber Sigurnost na Univerzitetu u Liverpoolu, Ujedinjeno Kraljevstvo i diplomirani je inžinjer elektrotehnike i računarstva na Univerzitetu u Sarajevu, Bosna i Hercegovina. Zanima se sa oblast digitalne forenzike i interdisciplinarnu primjenu cyber sigurnosti. U svom magisteriju, Lejla je razvila inovativan pristup digitalnoj forenzici namjenski za serverless cloud okruženja, primjenjujući blockchain tehnologiju i posebno razvijeni okvir za ekstrakciju i trajno čuvanje digitalnih dokaza u izvornom obliku. Osim akademskih postignuća, Lejla je uspješno realizirala velik broj profesionalnih kurseva u domeni računarske sigurnosti, upravljanja podacima i dizajna računarske infrastrukture.

Lejla je dobitnik prestižne Chevening stipendije za cyber sigurnost. Ponosna je članica Women4Cyber Bosna i Hercegovina, gdje djeluje kao stručnjak za sigurnosne tehnologije.

srdjan@smesecurity.ba

Srđan Rajčević, Specijalista cyber sigurnosti

Srđan Rajčević je specijalista cyber sigurnosti u kompaniji Sectreme gdje radi na poslovima analitičara malvera i reverznog inžinjera. Pored akademskih kvalifikacija (Magistar napredne cyber sigurnosti - King's College London, Diplomirani inžinjer računarstva - The University of Sheffield, Diplomirani pravnik - Univerzitet u Banjoj Luci, Magistar poslovnog prava - Univerzitet u Banjoj Luci) i CISSP certifikata, ima preko 16 godina radnog iskustva u javnom sektoru od čega 10 godina kao direktor Agencije za informaciono društvo RS i 4 godine kao ministar za naučnotehnološki razvoj, visoko obrazovanje i informaciono društvo u Vladi RS. Trenutno je angažovan i kao konsultant na poslovima izgradnje cyber kapaciteta u javnom i privatnom sektoru na području Zapadnog Balkana. Predmet užeg interesovanja mu je upotreba vještačke inteligencije u cyber operacijama. Dobitnik je Chevening nagrade za istraživanje polimorfičnog malvera.

Uvod

Digitalizacija je vjerovatno jedan od najvažnijih pojmova i trendova savremenog poslovanja. Ona donosi niz prednosti za poslovne subjekte, javne ustanove i fizička lica te prožima gotove sve naše aktivnosti - učenje i zabavu, rad, komunikaciju, zapošljavanje, poslovanje, plaćanje, i td. Digitalizacija nudi toliko mnogo moćnih obećanja, da joj se prilagođavaju poslovni procesi i načini rada, usvajaju se zakoni i mijenja infrastruktura, sve kako bi se ubrzao proces digitalizacije.

Poslovni subjekti i među njima mala i srednja preduzeća (SME) prepoznali su prednosti digitalizacije i mogućnosti koje ona donosi. Inovativni digitalni servisi nastavljaju pristizati 'kao sa trake', a njihova obećanja čine ih atraktivnim poslovnoj zajednici, i posebno SME. Veća produktivnost, niži troškovi poslovanja, pristup udaljenim tržištima, brža, neprekinuta i sadržajnija povezanost unutar i izvan organizacije sa saradnicima, klijentima, dobavljačima, tržištima i njihovim tehničkim resursima, bez obzira gdje se oni nalazili, su prihvaćeni s oduševljenjem. Lišeni tereta naslijeđa, krutih pravila i sporog odlučivanja, SME su u prednosti nad većim poslovnim subjektima u prilagođavanju digitalnom ambijentu. Oslanjajući se na agilnost, SME usvajaju digitalne tehnologije i nove načine rada, praktično u hodu. Osim toga, brojni digitalni servisi su besplatni što ih čini popularnim sa cjenovno osjetljivim subjektima kakvi su SME.

Zaposlenici SME odavno i redovno komuniciraju e-poštom, razmjenjuju poruke i online pozive preko digitalnih messenger platformi. Razmjenjuju informacije sa koleg-ic-ama, partnerima, dobavljačima i kupcima, pristupaju računarskim resursima unutar i izvan radnog vremena, sa radnog mjesta, od kuće ili sa udaljene lokacije, sa poslovnog ili privatnog računara ili mobitela. Nedostatak svijesti ili 'kulture' cyber sigurnosti može ih učiniti ležernim spram uređaja ili mreže koju koriste, softvera kojeg instaliraju ili linka kojeg slijede. K tome, promjene koje su nastale kao posljedica digitalizacije i pandemije, izbrisale su fizičke granice između privatnog i poslovnog života, fenomen kojem su posebno izloženi zaposlenici SME.

Privreda većine država zavisi od uspjeha SME, a pandemija nas je podsjetila na njihovu važnost. Štaviše, broj SME se povećava od početka milenija na ovamo i na globalnom nivou i u Evropi, u 2023. većina SMEs u EU su bila mikropreduzeća sa manje od 9 zaposlenih. Istodobno, SME su učestala meta cyber napada. Verizon-ov izvještaj pokazuje da je gotovo polovina napada ciljalo SME. Također, istraživanja o upotrebi interneta na Balkanu pokazuju kako su briga za cybersigurnost i online plaćanja tipični za zemlje Zapadnog Balkana. Razlog za učestale napade na SME su višestruki i imanentni ovom segmentu. Veća izloženost temeljem (nekritične) upotrebe proizvoda, ograničena raspoloživost materijalnih i kadrovskih resursa, nepostojanje kulture cybersigurnosti, neformalna organizacija uz manjak pravila i kontrole cyber aktivnosti korisnika u kombinaciji sa digitalizacijom i inovacijama na strani cyber kriminala, čine SME lak(š)im metama cyber napada.

Cyber otpornost organizacije ključna je za njenu stabilnost, reputaciju i održivost. Baš kao i mogućnosti koje digitalizacija otvara, cyber rizici su naša realnost. Cyber rizici ne smiju biti potcjenjeni, zanemareni niti jednokratno adresirani. Specifičnosti malih i srednjih preduzeća su prepoznate u industriji cyber sigurnosti i osmišljene su preporuke prilagođene primjeni u ambijentu SME. Dobre vijesti su kako pravovremenim i ciljanim djelovanjem SME mogu učiniti mnogo da materijalno poprave i kontinuirano unapređuju svoju cyber otpornost.

Ovaj vodič predstavlja našu pomoć malim i srednjim organizacijama u tome smjeru.

Definicije

Backdoor – Metoda koja omogućava pristup računarskim sistemima uz zaobilaženje standardnih sigurnosnih provjera

Backup – Rezervna kopija podataka

Dekripcija – Proces pretvaranja nerazumljivog oblika podataka u čitljive podatke korištenjem ključeva i metoda dekripcije.

Enkripcija – Proces pretvaranja čitljivih podataka u oblik koji je nerazumljiv korištenjem ključeva i metoda enkripcije. Cilj enkripcije je zaštita podataka od neovlaštenog pristupa.

IAM (Identity and Access Management) – Proces upravljanja identitetom i pristupom podacima koji omogućava pristup sistemima i podacima samo ovlaštenim korisnicima.

MFA (Multi Factor Authentication) – Metoda autentifikacije koja koristi više faktora prilikom provjere identiteta kao što su lozinka, sigurnosni kod ili token, te biometrijski podaci.

TLS (Transport Layer Security) – Sigurnosni protokol koji omogućava siguran prenos podataka preko mreže

VPN (Virtual Private Network) – Tehnologija koja omogućava kreiranje privatne komunikacije preko javne internet mreže.

Nulta tačka: Odabir pouzdanog partnera za cyber sigurnost

Važnost partnerstva: Odabir pravog partnera nije samo odluka o tehničkim resursima ili budžetu; to je strateški izbor koji može značajno utjecati na otpornost vaše organizacije prema cyber napadima i njen dugoročni uspjeh. Kompanije specijalizirane u domeni cyber sigurnosti i jakom reputacijom mogu vam pomoći u identifikaciji, evaluaciji i ublažavanju rizika kojima je vaša organizacija izložena.

Kriteriji za odabir:

1. **Reputacija:** Uspješan rad i preporuke cyber security kompanija mogu poslužiti kao pouzdan pokazatelj njihovih sposobnosti.
2. **Stručnost:** Kompanija bi trebala imati stručnjake specijalizirane za cyber sigurnost, posebno one fokusirane na industriju u kojoj vaša organizacija posluje.
3. **Dugovječnost:** Razmotrite potencijal kompanije da bude dugoročni partner. Cyber sigurnost nije jednokratan projekat, već kontinuirani proces.

Inicijalni sastanak i kratka analiza rizika: Kada identificirate potencijalne partnere, ključan je inicijalni sastanak kada treba urediti sljedeće:

1. **Strateško usklađivanje:** Uskladiti strateške ciljeve vaše organizacije s mogućnostima koje cyber security kompanija može implementirati.
2. **Kratka analiza rizika:** U ovoj fazi cilj je identificirati osnovne cyber sigurnosne rizike kojima je vaša organizacija izložena. Ovaj pregled će pomoći u razvoju preliminarnog plana za upravljanje rizicima.
3. **Prilagodba i fleksibilnost u implementaciji:** Iako ovaj vodič pruža korak-po-korak pristup, važno je priznati da svaka organizacija ne može napredovati linearnim putem kako je prikazano u Infografici. Organizacije će možda morati prilagoditi ove korake na temelju trenutnog stanja i prioritetnih oblasti.

Menadžment SME organizacija treba steći razumijevanje ključne uloge koju cyber security kompanije igraju i u suradnji s njima spoznati kako prilagoditi strategije cyber sigurnosti kako bi odgovarale jedinstvenom kontekstu njihove organizacije.

1. Upravljanje imovinom – Inventura resursa i sistema

Proces zaštite digitalne infrastrukture vaše organizacije započinje detaljnom inventurom resursa i sistema. Da biste učinkovito zaštititi svoju imovinu, morate tačno znati šta istu čini. Iako već možda imate popis inventara, sada je potrebno kreirati listu uređaja s potrebnim informacijama kako biste zaštitili sve aktivne komponente. Inicijativa za proces inventure treba doći od strane višeg menadžmenta ili biti odobrena od njega. Ovo daje organizacijski autoritet ovoj aktivnosti i osigurava usklađenost svih odjela.

Koraci implementacije

1. **Identifikacija imovine:** Kategorizirajte imovinu u različite tipove kao što su serveri, storage, mrežni uređaji, korisnički uređaji (desktop računari, laptopi itd.), mobilni uređaji (tableti, telefoni itd.), i IP-bazirani telefonski sistemi. Detalji uključeni u inventar zavise od veličine organizacije i složenosti mreže. Ključno je postići ravnotežu između iscrpnog popisa i operativne efikasnosti. Ne zaboravite na softverske resurse kao što su aplikacije, operativni sistemi, baze podataka itd. Popišite usluge na koje ste pretplaćeni, bilo da se radi o hostingu, emailu ili nekoj aplikaciji ili servisu. Prikupite informacije o infrastrukturnim uslugama koje koristite, poput pružatelja usluga interneta, telefonskih i DATA paketa.

2. **Alati za automatsko otkrivanje:** Moguće je da nemate urednu dokumentaciju o nabavljenim uređajima ili da vaši zaposlenici koriste vlastite uređaje za rad. Bez obzira na to, svi uređaji moraju biti evidentirani, kontrolirani i zaštićeni. Za kompromitaciju infrastrukture dovoljan je samo jedan uređaj kojem napadač može pristupiti. Stoga koristite alate za automatsko otkrivanje imovine koji skeniraju vašu mrežu i identificiraju povezane uređaje, kao što su Advanced IP Scanner, IP Address Manager, Angry IP Scanner ili slični alati. Pomoću ovih alata identificirajte uređaje na mreži koji nisu evidentirani na vašoj listi inventara.

3. **Odluke o kontroli pristupa:** Donosite odluke koje sprječavaju dodavanje uređaja u sistem bez specifičnog odobrenja od strane organizacije, čime ćete omogućiti pravovremenu zaštitu. Pobrinite se da budu do kraja provedene i da imate mehanizme zaštite od nepoštivanja.

4. **Dokumentacija:** Kreirajte listu inventara na sigurnoj lokaciji. Uključite atribute kao što su ime uređaja, tip, serijski broj, lokacija, dodijeljeni korisnik, IP adresa, MAC adresa, i operativni status. Na ovoj tački možete razmotriti korištenje softvera za upravljanje imovinom kao što su ManageEngine AssetExplorer ili Spiceworks, koji mogu pomoći u upravljanju hardverskim i softverskim inventarima.

5. **Redovno ažuriranje inventara:** Inventar imovine treba redovno ažurirati kako bi odražavao tačno stanje organizacije u svakom trenutku.

6. **Identifikacija zastarjele imovine:** Ključno je odmah ukloniti imovinu iz sistema koja se više ne može ažurirati, ali i dalje ima poznate ranjivosti. Takva imovina pruža lak pristup vašoj infrastrukturi i predstavlja visoki rizik za sigurnost sistema.

7. **Identifikacija nelegalnog softvera:** Budite sigurni da svaki komad takozvanog crack-ovanog softvera otvara „backdoor“ u vašu organizaciju. Onemogućite instalaciju nelegalnog softvera, jer vas takav softver na kraju košta mnogo više od legalnih kopija.
8. **Angažirajte stručnjake:** Potražite stručnjake koji posjeduju specijalizirano znanje da osigurate da je inventurna lista sveobuhvatna, a inventar pravilno klasificiran i praćen.

Zaključak: Upravljanje imovinom podrazumijeva uspostavu i održavanje tačnih i ažurnih informacija o vašim sistemima i resursima, koji vam omogućavaju obavljanje svakodnevnih aktivnosti i donošenje informiranih odluka. Tokom vremena, kroz razvoj organizacije, sistemi rastu i mijenjaju su i često može biti izazovno održati vjerodostojno stanje digitalne infrastrukture organizacije. Korištenje alata za automatsko otkrivanje imovine, uklanjanje zastarjelih resursa, kategorizacija imovine, te redovno ažuriranje inventara važni su koraci koje organizacija treba sprovoditi, a što će omogućiti efikasniju zaštitu od sigurnosnih prijetnji i incidenata.

2. Klasifikacija podataka i nivoi odgovornosti

Važnost klasifikacije podataka i definisanja nivoa odgovornosti ne može se dovoljno naglasiti u savremenoj strategiji zaštite informacija. Ona vam omogućava primjenu odgovarajućeg nivoa sigurnosti za svaku vrstu podataka, čime se poboljšava upravljanje podacima. Također, jasno definirane uloge i odgovornosti su ključne kako bi se osiguralo da odgovarajuće osobe imaju pristup podacima i da je jasno pod kojim okolnostima im je taj pristup omogućen.

Koraci implementacije

1. **Identifikacija i katalogizacija podataka:** Identificirajte i katalogizirajte vrste podataka kojima upravljate, kao što su zapisi o zaposlenicima, finansijske informacije, ugovori, podaci o klijentima i intelektualna svojina.
2. **Kriteriji za klasifikaciju:** Razvijte kriterije za klasifikaciju podataka na osnovu njihove osjetljivosti i važnosti za organizaciju. Uobičajeni četverostepeni sistem je: Javni, Interna upotreba, Osjetljivi i Visoko osjetljivi.
3. **Označavanje podataka:** Implementirajte mehanizme za označavanje podataka prema njihovoj klasifikaciji koristeći alate kao što su: Microsoft Azure Information Protection, posebno zanimljiv za korisnike Microsoft 365, ili Adobe Acrobat Pro. Konsultujte stručnjake za cyber sigurnost. Vaš izbor rješenja zavisi ne samo od budžeta kojim raspolažete, već i od ostalih komponenti sistema koje ste ranije implementirali.
4. **Uloge i odgovornosti:** Jasno definišite ko je odgovoran za koje podatke. Koristite opise poslova kao vodič, ali se također konsultirajte s rukovodiocima odjela kako biste potvrdili praktične svakodnevne potrebe za podacima. Obezbijedite da su zaposlenicima dodijeljena samo ona prava koja im omogućavaju da obavljaju svoje redovne aktivnosti, kako bi se spriječila eventualna slučajna ili namjerna zloupotreba.
5. **Privremene (Just-in-Time/Just-Enough) privilegije:** Implementirajte sistem koji korisnicima daje minimalne potrebne privilegije za obavljanje zadataka u datom trenutku, koristeći alate kao što su Microsoft Azure Active Directory ili AWS IAM. U našem regionu, CyberArk i One Identity su također popularni.
6. **Audit i monitoring:** Važno je uvesti procese za audit i monitoring ovih aktivnosti i kontrola. Koristite alate za nadzor kako biste zabilježili ko je pristupio kojim podacima i kada. Postavite alarme za neovlaštene ili sumnjive pokušaje pristupa.

Zaključak: Klasifikacija podataka i uspostavljanje nivoa odgovornosti su osnovni aspekti upravljanja cyber sigurnošću. Oni djeluju kao temelj na kojem se grade politike upravljanja podacima i kontrole pristupa, čime se olakšava operativna efikasnost i sigurnost. Kroz sistematsku implementaciju ovih koraka i periodičnu reviziju, menadžment malih i srednjih preduzeća može uspostaviti otpornu i prilagodljivu poziciju prema cyber sigurnosti.

3. Upravljanje rizicima

Preuzimanje rizika je neizbježan dio poslovanja, ali učinkovito upravljanje rizicima omogućava bolje donošenje odluka, optimizaciju resursa i dugoročnu zaštitu organizacije. U okviru upravljanja rizicima, cilj organizacije je da metodološki identificira rizike i imovinu koja im je izložena, procijeni izglednost nastanka negativnog ishoda i valorizira potencijalnu štetu, te primjeni mjere koje će umanjiti mogućnost nastanka štete kao i samu štetu. Upravljanje rizicima organizacijama donosi mogućnosti informiranog i boljeg odlučivanja, te stvara pretpostavke za dinamičan odgovor organizacije na promjene okolnosti i riziko-profila.

Koraci implementacije

1. **Izbor metodologije:** Prvi korak u upravljanju rizicima je odabir odgovarajuće metodologije koja najbolje odgovara specifičnostima vaše organizacije. Organizacije se razlikuju po veličini, djelatnosti, strukturi i rizicima s kojima se suočavaju. Za većinu malih i srednjih preduzeća (SME), komponentni pristup je najprikladniji. Ovaj pristup omogućava fokus na pojedinačne dijelove imovine (kao što su serveri, računari, softver, mrežni uređaji) te omogućava preciznu identifikaciju i rangiranje rizika vezanih uz svaku komponentu. S druge strane, organizacije s kompleksnijom strukturom mogu razmotriti sistemski pristup, koji integrira procjenu rizika u kontekstu šireg poslovnog okruženja.

2. **Identifikacija i analiza rizika:** Identifikacija rizika uključuje prepoznavanje svih potencijalnih prijetnji koje bi mogle ugroziti imovinu ili operativne procese organizacije. Nakon identifikacije slijedi analiza rizika koja procjenjuje vjerovatnoću njihovog ostvarenja i moguću štetu koju bi mogli prouzrokovati. Ovo se često postiže putem izrade matrice rizika koja omogućava vizualizaciju rizika po prioritetima, od onih s najvećim potencijalnim utjecajem do onih s manjim utjecajem. U ovoj fazi, organizacija može koristiti različite alate i softverska rješenja za procjenu rizika, što olakšava donošenje informiranih odluka.

3. **Primjena kontrola:** Nakon identifikacije i analize, organizacija treba implementirati odgovarajuće kontrole koje smanjuju rizik na prihvatljiv nivo. Kontrole mogu biti preventivne, detektivne ili korektivne, ovisno o prirodi rizika. Važno je da kontrole budu proporcionalne riziku kojem su namijenjene, kako bi bile efikasne, ali i ekonomski opravdane. Primjeri kontrola uključuju instalaciju antivirusnog softvera, redovno pravljenje sigurnosnih kopija podataka, segmentaciju mreže, te obuku zaposlenika o sigurnosnim politikama. Pored tehničkih kontrola, organizacija treba razviti politike i procedure koje podržavaju kontinuirano upravljanje rizicima.

4. **Rezidualni rizik:** Bez obzira na implementirane kontrole, uvijek ostaje određeni nivo rizika koji se ne može potpuno eliminirati – poznat kao rezidualni rizik. Ključno je da organizacija bude svjesna ovog rizika i da ga ocijeni kao prihvatljiv za poslovanje. Ako rezidualni rizik prelazi prihvatljivi nivo, organizacija može razmotriti dodatne mjere, kao što su osiguranje ili prijenos rizika na treću stranu putem outsourcinga. Važno je napomenuti da su opcije za prijenos rezidualnog rizika putem osiguranja ograničene na određenim tržištima, pa je ključno procijeniti dostupnost takvih opcija na lokalnom nivou.

5. **Redovna revizija rizika:** Upravljanje rizicima nije jednokratan proces, već zahtijeva kontinuiranu pažnju i prilagođavanje. Riziko profil organizacije može se promijeniti zbog novih tehnologija, promjena u poslovnim procesima, promjena u zakonodavstvu ili vanjskih prijetnji poput novih cyber napada. Stoga je neophodno redovno provoditi reviziju rizika i kontrola, posebno nakon značajnih promjena u imovini ili dobavljačima, te minimalno jednom godišnje. Ova revizija omogućava organizaciji da osigura da su implementirane kontrole i dalje efikasne te da se rezidualni rizik drži unutar prihvatljivih granica.

Zaključak: Upravljanje rizicima je ključni element za održavanje sigurnosti, stabilnosti i otpornosti organizacije na izazove. Pravilna implementacija i redovno revidiranje strategija upravljanja rizicima omogućava organizaciji da se efikasno suoči s promjenama, prilagodi novim okolnostima i zaštiti svoje ključne resurse. Kontinuirani nadzor i prilagodba procesa upravljanja rizicima osiguravaju da organizacija ostane proaktivna u suočavanju s potencijalnim prijetnjama, što doprinosi dugoročnom uspjehu i održivosti.

4. Upravljanje identitetom i pristupom (Identity and Access Management - IAM)

Upravljanje identitetom i pristupom (IAM) je ključan element u zaštiti digitalnih resursa organizacije, osiguravajući da samo ovlašteni korisnici imaju pristup određenim sistemima, podacima ili funkcionalnostima. Ova praksa je od vitalnog značaja za smanjenje rizika od neovlaštenog pristupa, krađe podataka ili drugih sigurnosnih incidenata.

Koraci implementacije

1. **Izrada politike pristupa:** Prvi korak u procesu upravljanja identitetom i pristupom je razvoj jasne i sveobuhvatne politike koja definira ko treba imati pristup kojim sistemima, podacima ili funkcionalnostima, kao i razloge i uvjete pod kojima se taj pristup odobrava. Ova politika treba biti dosljedna i primjenjiva u cijeloj organizaciji, osiguravajući da svi korisnici imaju odgovarajući nivo pristupa u skladu sa svojim ulogama i odgovornostima.

2. **Upravljanje korisničkim računima:** Uključite detaljnu politiku za upravljanje korisničkim računima koja pokriva "novopridošle, prelazne i odlazeće" korisnike. Ova politika osigurava da se prava pristupa dodjeljuju, prilagođavaju ili ukidaju u skladu s promjenama u ulogama zaposlenika. Redovno ažuriranje pristupnih prava sprječava prekomjerni pristup i smanjuje rizik od neovlaštenog korištenja starih ili nepotrebnih naloga.

3. **Uklanjanje privremenih korisničkih računa:** Privremeni korisnički računi se često koriste za specifične zadatke ili projekte. Važno je osigurati da se ovi korisnički računi uklanjaju ili suspendiraju čim više nisu potrebni, kako bi se spriječilo njihovo korištenje za neovlašteni pristup nakon završetka zadatka ili projekta.

4. **Višefaktorska autentifikacija (Multi Factor Authentication - MFA):** Višefaktorska autentifikacija (MFA) je ključna za dodatno osiguranje korisničkih računa. Implementacijom višefaktorske autentifikacije, organizacija zahtijeva od korisnika da prođu kroz dodatne slojeve provjere identiteta, kao što su sigurnosni kodovi, biometrijski podaci ili fizički tokeni, uz standardnu lozinku. Ova dodatna zaštita značajno smanjuje rizik od kompromitacije korisničkih računa.

5. **Odabir tipova autentifikacije:** Birajte različite tipove autentifikacionih faktora u zavisnosti od nivoa sigurnosti potrebnog za određeni sistem ili podatke. Na primjer, za kritične sisteme može biti potrebna kombinacija lozinke i biometrijske autentifikacije, dok za manje osjetljive sisteme može biti dovoljna samo lozinka uz sigurnosni kod.

6. **Monitoring i auditing:** Implementirajte robustan sistem za kontinuirano praćenje i analiziranje pokušaja pristupa. Ovaj sistem treba automatski identificirati sumnjive aktivnosti, poput neuspjelih pokušaja prijave ili pristupa iz neočekivanih geografskih lokacija, te odmah pokrenuti odgovarajuće protokole za odgovor, kao što su obavještavanje nadležnih osoba ili privremeno zaključavanje korisničkog računa.

Zaključak: Upravljanje identitetom i pristupom predstavlja temeljnu sigurnosnu praksu koja štiti organizaciju od neovlaštenog pristupa i potencijalnih sigurnosnih incidenata. Pravilna implementacija IAM politike, u kombinaciji s redovnim praćenjem i ažuriranjem korisničkih računa, omogućava organizaciji da održi visoke standarde sigurnosti i efikasno upravlja rizicima povezanim s digitalnim resursima.

5. Upravljanje uređajima i ranjivostima

Upravljanje uređajima i ranjivostima ključno je za održavanje sigurnosti informatičkog okruženja organizacije. Ovi procesi osiguravaju da svi uređaji u mreži budu pravilno nadzirani, ažurirani i zaštićeni, te da se potencijalne ranjivosti brzo identificiraju i otklone.

Koraci implementacije

1. **Upravljanje uređajima:**
    - **Jedinstvena platforma za upravljanje:** Koristite jedinstvenu platformu za upravljanje svim uređajima unutar organizacije. Ova platforma treba nadzirati sve uređaje kako bi se osiguralo da su u skladu sa sigurnosnim standardima organizacije. Centralizovano upravljanje olakšava praćenje i održavanje sigurnosnih politika te omogućava brzu reakciju na potencijalne prijetnje.
    - **Katalogizacija uređaja:** Svi uređaji trebaju biti katalogizirani s relevantnim informacijama kao što su model uređaja, operativni sistem, i mrežne privilegije pristupa. Ovaj katalog omogućava organizaciji da ima potpuni pregled nad svim uređajima u mreži, čime se olakšava identifikacija eventualnih ranjivosti ili neusklađenosti sa sigurnosnim standardima.
    - **Standardizirane sigurnosne konfiguracije:** Održavajte standardizirane sigurnosne konfiguracije na svim uređajima kako biste minimizirali rizike od ranjivosti. Standardizacija uključuje implementaciju postavki kao što su sigurnosne politike za lozinke, enkripcija podataka, i pravila za ažuriranje softvera. Ove konfiguracije trebaju biti dosljedno primijenjene na sve uređaje kako bi se smanjio rizik od sigurnosnih propusta.
2. **Upravljanje Ranjivostima:**
    - **Brza identifikacija ranjivosti:** Redovno provodite automatizovane preglede sistema ili koristite izvještaje trećih strana kako biste brzo identificirali nove ranjivosti. Automatizirani alati za skeniranje ranjivosti omogućavaju organizaciji da pravovremeno otkrije potencijalne prijetnje i odmah započne s njihovim otklanjanjem.
    - **Procjena rizika:** Nakon identifikacije, svaka ranjivost treba biti procijenjena prema riziku koji predstavlja, uzimajući u obzir potencijalni uticaj na organizaciju i vjerovatnoću da će ranjivost biti iskorištena. Ova procjena pomaže u određivanju koje ranjivosti zahtijevaju hitnu pažnju i resurse za sanaciju.
    - **Prioritetizacija ranjivosti:** Na osnovu procjene rizika, rangirajte ranjivosti prema njihovoj ozbiljnosti kako biste omogućili ciljano ublažavanje. Fokusirajte se na otklanjanje ranjivosti s najvišim rizikom, koje predstavljaju najveću prijetnju za sigurnost organizacije.

Zaključak: Upravljanje uređajima i ranjivostima ključni su aspekti u održavanju sigurnosnog integriteta organizacije. Pravilno upravljanje uređajima osigurava da svi sistemi budu u skladu s

organizacijskim sigurnosnim standardima, dok učinkovito upravljanje ranjivostima omogućava pravovremeno otkrivanje i otklanjanje sigurnosnih prijetnji. Kroz dosljednu primjenu ovih principa, organizacija može značajno smanjiti rizik od cyber napada i osigurati kontinuiranu zaštitu svojih digitalnih resursa.

6. Kontinuirana nadogradnja i ažuriranje

Redovno ažuriranje sistema i softvera ključan je korak u održavanju sigurnosti organizacije. Kontinuirane nadogradnje i ažuriranja osiguravaju da su svi uređaji zaštićeni od najnovijih prijetnji, dok se istovremeno unapređuje performanse i funkcionalnost sistema.

Koraci implementacije

1. **Automatizirana ažuriranja:** Gdje god je moguće, omogućite automatska ažuriranja za sve uređaje i softverske aplikacije. Automatizacija ažuriranja smanjuje rizik od ljudske greške i osigurava da su svi uređaji redovno osvježeni s najnovijim sigurnosnim zakrpama i nadogradnjama. Ovo uključuje operativne sisteme, antivirusni softver, web pretraživače, i druge ključne aplikacije koje koriste vaši zaposlenici.

2. **Ručno ažuriranje uređaja:** Za uređaje i aplikacije kod kojih nije moguće omogućiti automatsko ažuriranje, postavite redovan raspored za ručna ažuriranja. Ovo može uključivati specifične aplikacije ili prilagođene sisteme koji zahtijevaju pažljivo testiranje prije implementacije novih verzija. Ključno je osigurati da su svi uređaji redovno provjeravani i da su ažuriranja primijenjena u najkraćem mogućem roku kako bi se spriječile potencijalne sigurnosne prijetnje.

3. **Praćenje statusa ažuriranja:** Implementirajte sistem za nadzor statusa ažuriranja na svim uređajima u mreži. Ovaj sistem treba biti u mogućnosti da otkrije bilo kakve neuspjele pokušaje ažuriranja ili uređaje koji nisu ažurirani u predviđenom vremenskom okviru. Redovno praćenje omogućava brzo prepoznavanje i otklanjanje problema, čime se smanjuje rizik od ranjivosti.

4. **Reakcija na neuspjela ažuriranja:** Kada se detektiraju neuspjeli pokušaji ažuriranja, odmah poduzmite korake kako biste otklonili problem. To može uključivati ručno ponovno pokretanje procesa ažuriranja, kontaktiranje tehničke podrške, ili identifikaciju i uklanjanje bilo kojih prepreka koje su spriječile uspješno ažuriranje.

Zaključak: Kontinuirane nadogradnje i ažuriranja ključni su za zaštitu informatičke infrastrukture organizacije od novih prijetnji i ranjivosti. Automatska ažuriranja olakšavaju održavanje sigurnosti, dok ručno ažuriranje osigurava da čak i specijalizirani sistemi ostanu zaštićeni. Redovno praćenje i brza reakcija na neuspjele pokušaje ažuriranja dodatno osiguravaju da svi uređaji ostanu ažurirani i sigurni.

7. Rad na daljinu - Zaštita

S obzirom na sve veću prisutnost rada na daljinu, zaštita radnika koji rade izvan kancelarije postaje ključna za očuvanje sigurnosti organizacije. Implementacija odgovarajućih sigurnosnih protokola osigurava da pristupanje resursima organizacije s udaljenih lokacija ostane sigurno i zaštićeno od potencijalnih prijetnji.

Koraci implementacije

1. **Sigurnosni protokoli za rad na daljinu:** Koristite VPN (Virtual Private Network) rješenja za enkripciju saobraćaja između korisnika i organizacije. VPN osigurava da sav podatkovni promet ostane nevidljiv neovlaštenim entitetima, čak i ako se koristi javna ili nesigurna mreža. Time se smanjuje rizik od prisluškivanja ili krađe podataka dok radnici pristupaju sistemima i podacima organizacije s udaljenih lokacija.
2. **Višefaktorska autentifikacija (MFA):** Implementirajte višefaktorsku autentifikaciju (MFA) kao dodatni sloj sigurnosti prilikom pristupanja resursima organizacije s udaljenih lokacija. MFA zahtijeva od korisnika da, uz unos lozinke, prođe i dodatni sigurnosni korak, kao što je unos sigurnosnog koda, biometrijska provjera ili upotreba sigurnosnog tokena. Ovaj dodatni sloj zaštite značajno smanjuje mogućnost neovlaštenog pristupa, čak i ako je osnovna lozinka kompromitirana.
3. **Kontinuirano praćenje i upozorenja:** Implementirajte sisteme za kontinuirano praćenje i analiziranje aktivnosti radnika na daljinu. Ovi sistemi trebaju biti u mogućnosti identificirati sumnjive aktivnosti, kao što su pokušaji pristupa s neovlaštenih ili neočekivanih lokacija, te odmah pokrenuti odgovarajuće protokole za odgovor, uključujući slanje upozorenja nadležnim osobama ili privremeno onemogućavanje pristupa kritičnim resursima.

Zaključak: Zaštita radnika na daljinu je ključna za održavanje sigurnosti organizacije u modernom poslovnom okruženju. Korištenje VPN rješenja, implementacija višefaktorske autentifikacije i kontinuirano praćenje aktivnosti na daljinu osiguravaju da pristupanje resursima organizacije ostane sigurno, bez obzira na lokaciju korisnika. Pravilna implementacija ovih mjera omogućava organizaciji da zaštiti svoje podatke i sisteme, čak i kada se rad obavlja izvan ureda.

8. Sigurnost podataka

Zaštita podataka je od ključne važnosti za očuvanje integriteta, povjerljivosti i dostupnosti informacija unutar organizacije. Pravilna implementacija mjera sigurnosti osigurava da su podaci zaštićeni tokom prenosa, dok su pohranjeni, i da im pristupaju samo ovlašteni korisnici.

Koraci implementacije

1. **Zaštita podataka u prenosu:** Osigurajte da su svi podaci koji se prenose između korisnika i sistema organizacije zaštićeni kako bi se spriječilo neovlašteno pregledanje ili izmjena. Korištenje sigurnosnih protokola kao što su TLS (Transport Layer Security) i VPN (Virtual Private Network) rješenja omogućava enkripciju podataka u prijenosu, čime se smanjuje rizik od presretanja ili manipulacije podacima dok se prenose putem mreže.
2. **Zaštita pohranjenih podataka:** Osigurajte da su svi pohranjeni podaci zaštićeni (podaci u mirovanju). Korištenje enkripcije za pohranjene podatke osigurava da, čak i ako neovlašteni korisnik pristupi fizičkim ili digitalnim medijima, podaci ostanu nečitljivi bez odgovarajućih ključeva za dekripciju.
3. **Fizičke i logičke kontrole pristupa:** Implementirajte fizičke i logičke kontrole pristupa kako biste osigurali da samo ovlašteni korisnici mogu pristupiti i/ili mijenjati vaše podatke. Fizičke kontrole uključuju ograničeni pristup serverima i drugim uređajima, dok logičke kontrole uključuju autentifikaciju i autorizaciju na aplikativnom nivou. Pristup podacima treba biti ograničen na osnovu principa najmanjeg privilegija, što znači da korisnici imaju samo ona prava koja su im potrebna za obavljanje njihovih zadataka.
4. **Korištenje standardiziranih kriptografskih algoritama:** Koristite aktuelne standardizirane kriptografske algoritme za zaštitu podataka. Algoritmi poput AES i RSA osiguravaju visok nivo zaštite podataka od neovlaštenog pristupa. Važno je redovno pratiti razvoj sigurnosnih protokola i algoritama te ažurirati korištene metode kako bi se osigurala dugoročna zaštita.
5. **Evidencija i praćenje pristupa podacima:** Logirajte sve pristupe podacima i redovno pratite aktivnosti kako biste otkrili neobične upite, pokušaje masovnog izvoza podataka ili neovlašteni administrativni pristup. Ova evidencija omogućava brzo prepoznavanje mogućih kompromitacija i pokretanje odgovarajućih protokola za odgovor. Alati za praćenje i analizu logova mogu pomoći u otkrivanju sumnjivih aktivnosti u realnom vremenu.

Zaključak: Sigurnost podataka zahtijeva sveobuhvatan pristup koji uključuje zaštitu podataka u prijenosu, pohrani i ograničavanje pristupa samo na ovlaštene korisnike. Korištenjem standardiziranih kriptografskih metoda, implementacijom kontrola pristupa i kontinuiranim praćenjem pristupa podacima, organizacija može osigurati integritet, povjerljivost i dostupnost svojih informacija, te minimizirati rizik od kompromitacije podataka.

9. Rezervne kopije podataka (Backup)

Pravilno upravljanje rezervnim kopijama podataka ključno je za očuvanje kontinuiteta poslovanja i zaštitu od gubitka podataka uslijed tehničkih kvarova, cyber napada ili drugih nepredviđenih događaja. Implementacija backup strategije osigurava da se ključni podaci uvijek mogu obnoviti u slučaju incidenta.

Koraci implementacije

1. **Osiguranje ključnih podataka:** Osigurajte da svi podaci koji su ključni za funkcionisanje organizacije, uključujući poslovne podatke i konfiguracijske podatke, budu redovno kopirani. Ove rezervne kopije treba uključivati sve kritične informacije koje su neophodne za obnavljanje poslovnih operacija u slučaju gubitka podataka.
2. **3-2-1 Backup strategija:** Slijedite 3-2-1 strategiju kako biste osigurali višestruke rezervne kopije važnih datoteka koje su pohranjene na različitim lokacijama. Ova strategija uključuje:
    - Posjedovanje najmanje 3 kopije podataka.
    - Pohranjivanje tih kopija na najmanje 2 različita uređaja.
    - Posjedovanje 1 kopije koja se nalazi izvan lokacije organizacije (offsite), što dodatno štiti podatke od lokalnih katastrofa.
3. **Politika zadržavanja rezervnih kopija:** Definišite period zadržavanja za rezervne kopije, u skladu s poslovnim i regulatornim zahtjevima. Zadržavanje rezervnih kopija za određeni period omogućava vraćanje na ranije verzije podataka ako dođe do grešaka ili neželjenih izmjena u novijim kopijama.
4. **Politika rotacije rezervnih kopija:** Implementirajte politiku rotacije rezervnih kopija kako biste očuvali najnovije i najvažnije podatke. Rotacija rezervnih kopija osigurava da starije kopije budu redovno zamijenjene novijim verzijama, čime se smanjuje potreba za skladištenjem velikih količina podataka i osigurava dostupnost najrelevantnijih informacija.
5. **Redovno testiranje rezervnih kopija:** Redovno testirajte rezervne kopije kako biste osigurali da proces vraćanja podataka iz kopija funkcioniše ispravno. Ovo testiranje treba uključivati simulacije obnavljanja podataka kako bi se osiguralo da su svi potrebni koraci poznati i da sistem može brzo i efikasno obnoviti podatke u slučaju potrebe.
6. **Ograničavanje pristupa:** Ograničite pristup serverima koji se koriste za backup podataka. Samo ovlaštene osobe trebaju imati pristup ovim kritičnim resursima kako bi se smanjio rizik od neovlaštenog pristupa, krađe ili kompromitacije sigurnosnih kopija.

Zaključak: Upravljanje rezervnim kopijama podataka je vitalan dio strategije zaštite podataka. Korištenje 3-2-1 strategije, definiranje politike zadržavanja i rotacije, redovno testiranje rezervnih kopija i ograničavanje pristupa ključnim resursima osigurava da vaša organizacija može brzo i efikasno odgovoriti na gubitak podataka i očuvati kontinuitet poslovanja.

10. Logiranje i monitoring

Logiranje i monitoring su ključni za pravovremeno otkrivanje i reagiranje na sigurnosne incidente unutar organizacije. Pravilno konfigurirani i zaštićeni logovi omogućavaju detaljnu analizu događaja, identificiranje prijetnji i prevenciju budućih incidenata.

Koraci implementacije

1. **Omogućavanje logiranja:** Omogućite logiranje u svim kritičnim sistemima i aplikacijama kako biste osigurali da su svi relevantni događaji zabilježeni. Ovi zapisi omogućavaju detaljnu analizu u slučaju sigurnosnog incidenta, pružajući uvid u vrijeme, vrstu aktivnosti i korisnika koji je pokrenuo određene akcije.
2. **Pohrana i pristup logovima:** Osigurajte da znate gdje se logovi pohranjuju i kako im pristupiti. Centralizovana pohrana logova, uz korištenje sigurnih servera ili cloud rješenja, omogućava lakše upravljanje, pretraživanje i analiziranje zapisa. Jasno definisani procesi za pristup logovima su ključni za brzu reakciju u slučaju potrebe.
3. **Zaštita prenosa logova:** Kada se logovi šalju na centralizovanu lokaciju, koristite transportnu enkripciju kako biste osigurali da podaci budu zaštićeni tokom prenosa. Korištenje protokola poput TLS (Transport Layer Security) sprječava neovlaštene entitete da presretnu ili manipuliraju logovima dok se prenose kroz mrežu.
4. **Zaštita logova od manipulacije:** Implementirajte sigurnosne mjere koje štite logove od manipulacije ili neovlaštenih izmjena. To uključuje ograničavanje pristupa logovima samo ovlaštenim korisnicima i korištenje tehnologija za otkrivanje bilo kakvih pokušaja mijenjanja ili brisanja logova. Sigurni sistemi za arhiviranje logova pomažu u očuvanju integriteta zapisa.
5. **Detekcija i upozorenja:** Postavite upozorenja bazirana na očekivanim prijetnjama i neobičnim aktivnostima zabilježenim u logovima. Ova upozorenja omogućavaju brzu detekciju potencijalnih sigurnosnih incidenata, kao što su pokušaji neovlaštenog pristupa, masovni izvoz podataka ili neuobičajena aktivnost korisnika, te omogućavaju pravovremeno reagiranje kako bi se smanjila šteta.

Zaključak: Logiranje i monitoring su osnovni alati za otkrivanje i odgovaranje na sigurnosne prijetnje unutar organizacije. Omogućavanjem logiranja, osiguranjem sigurnosti logova tokom prenosa i pohrane, te postavljanjem detekcijskih upozorenja, organizacija može efikasno pratiti svoje sisteme, brzo prepoznati i reagirati na sigurnosne incidente, te zaštititi svoje digitalne resurse.

11. Upravljanje incidentima

Upravljanje incidentima je ključan dio strategije cyber sigurnosti, koji osigurava da organizacija može brzo i efikasno reagirati na sigurnosne prijetnje i incidente. Priprema i implementacija odgovarajućeg plana odgovora na incidente pomaže u minimiziranju štete, zaštiti podataka i očuvanju povjerenja klijenata.

Koraci implementacije

1. **Priprema plana odgovora na incidente:** Pripremite sveobuhvatan plan odgovora na incidente koji detaljno opisuje korake koje treba poduzeti u slučaju sigurnosnog incidenta. Plan treba biti fleksibilan i prilagodljiv različitim vrstama prijetnji, uključujući cyber napade, curenje podataka, ili neovlašteni pristup.
2. **Uključivanje pravih ljudi kroz formiranje tima:** Osigurajte da su u plan uključeni svi relevantni članovi tima, uključujući IT sigurnosni tim, pravni odjel, ljudske resurse, tim za odnose s javnošću, dobavljače i partnere, te viši menadžment. Svaki član tima treba imati jasno definirane odgovornosti u slučaju incidenta.
3. **Imenovanje odgovornih osoba:** Imenovanje specifičnih pojedinaca za rukovođenje incidentima je ključno. Ove osobe trebaju biti odgovorne za koordinaciju odgovora na incident, donošenje ključnih odluka i komunikaciju unutra izvan organizacije.
4. **Kriteriji za eskalaciju incidenta:** Uspostavite jasne kriterije za eskalaciju incidenta prema višem menadžmentu. To uključuje definisanje pragova ozbiljnosti incidenta, kao što su uticaj na poslovanje, povreda sigurnosti podataka, ili potreba za pravnim ili regulatornim prijavljivanjem.
5. **Pravni i regulatorni zahtjevi:** Osigurajte da plan uključuje osnovne smjernice o pravnim ili regulatornim zahtjevima za prijavljivanje incidenta. To može uključivati obavezu prijavljivanja povrede podataka nadležnim tijelima ili obavještavanje oštećenih strana u skladu s važećim zakonodavstvom.
6. **Transparentna komunikacija sa uposlenicima i kupcima:** Tokom incidenta, važno je održavati transparentnu i pravovremenu komunikaciju s uposlenicima i kupcima. Ova komunikacija treba pružiti jasne informacije o incidentu, poduzetim mjerama, i eventualnim koracima koje korisnici trebaju poduzeti.
7. **Evidencija incidenta:** Vodite pažljiv zapis o cijelom procesu odgovora na incident, uključujući donesene odluke, poduzete akcije, prikupljene podatke (ili nedostatke u podacima). Ova evidencija je važna za analizu nakon incidenta i za pravne ili regulatorne svrhe.
8. **Učenje iz incidenata:** Uključite lekcije naučene iz incidenata u buduća unapređenja plana i sigurnosnih procedura. Redovno revidirajte i ažurirajte plan na osnovu iskustava iz stvarnih incidenata kako bi se poboljšala sposobnost organizacije da se nosi s budućim prijetnjama.

9. **Vježbanje odgovora na incidente:** Redovno provodite vježbe odgovora na incidente koristeći alate koji pomažu organizaciji da testira i prakticira svoj odgovor na različite vrste cyber napada. Ove vježbe trebaju obuhvatiti sve potrebne aktivnosti, od postavljanja i planiranja do implementacije i aktivnosti nakon vježbe.

Zaključak: Upravljanje incidentima zahtijeva temeljitu pripremu i koordinaciju svih relevantnih resursa unutar organizacije. Pravilno osmišljen plan odgovora na incidente, uz redovne vježbe i revizije, omogućava organizaciji da efikasno reagira na sigurnosne prijetnje, minimizira štetu i brzo se oporavi od incidenata.

12. Obuka i podizanje svijesti o cyber sigurnosti

U modernom poslovnom okruženju, tehnologija često dominira raspravama o cyber sigurnosti, stvarajući dojam da su sigurnosna pitanja isključivo tehničke prirode i ograničena na IT osoblje. Međutim, ovakav pristup je površan i može dovesti do ozbiljnih propusta. Ljudi, a ne samo tehnologija, moraju biti u središtu strategije cyber sigurnosti svake organizacije, posebno malih i srednjih preduzeća (SME). Zaposlenici su često prva linija odbrane, ali i najslabija karika kada su nepripremljeni. Stoga je ključno razvijati sveobuhvatan program obuke i podizanja svijesti koji uključuje sve zaposlenike, od uprave do portira.

Koraci implementacije

1. **Planiranje i razvoj programa obuke:**
    - **Sveobuhvatni program:** Razvijte sveobuhvatan program obuke koji je prilagodljiv i ažuriran s najnovijim prijetnjama i taktikama koje koriste napadači. Ovaj program treba obuhvatiti sve aspekte cyber sigurnosti relevantne za organizaciju, uključujući osnovna znanja za sve zaposlenike i specijalizirane treninge za određene grupe.
    - **Kreativni pristup:** Kako biste povećali angažman, koristite kreativne metode poput postera, tematskih igara, društvenih objava i newslettera za popularizaciju programa. Ovi alati pomažu u održavanju interesa i povećavaju svijest o sigurnosnim rizicima na pristupačan način.
2. **Redovno testiranje i procjena:**
    - **Testiranje efikasnosti:** Provodite redovno testiranje i procjenu kako biste izmjerili efikasnost programa obuke. Ovo uključuje kvizove, simulacije napada i procjene u stvarnom radnom okruženju. Na osnovu rezultata, ažurirajte i poboljšavajte trening materijale.
    - **Ažuriranje materijala:** Administrator obuke treba redovno ažurirati materijale kako bi ostali relevantni u odnosu na nove prijetnje i načine napada. Razumijevanje izloženih tema treba biti provjereno među zaposlenima, a uspješni rezultati mogu biti simbolično nagrađeni kako bi se podstaklo učešće.
3. **Analiza incidenta kao dio obuke:** Uključite analizu stvarnih i simuliranih cyber incidenata u obuku. Ova analiza treba obuhvatiti način napada, odgovor organizacije i konačni ishod, te šta je bilo uspješno, a šta treba unaprijediti. Ovaj pristup pomaže u izgradnji kulture otvorenosti i kontinuiranom poboljšanju sigurnosnih praksi.
4. **Uključivanje uprave u edukativne programe:** Osigurajte da i uprava aktivno sudjeluje u edukativnim programima. Njihovo sudjelovanje ne samo da podiže nivo svijesti, već i pokazuje važnost cyber sigurnosti unutar cijele organizacije. Uprava treba biti primjer ostalim zaposlenicima i podržavati inicijative za podizanje svijesti i obuku.
5. **Redovne simulacije i praktične vježbe:** Redovno provodite simulacije i praktične vježbe kako bi organizacija bila spremna za stvarne cyber napade. Ove vježbe trebaju obuhvatiti

sve faze od planiranja do post-incident aktivnosti, omogućujući zaposlenicima da testiraju svoje vještine u kontroliranim uvjetima.

Zaključak: Obuka i podizanje svijesti o cyber sigurnosti moraju biti kontinuiran proces koji uključuje sve zaposlenike, bez izuzetka. Pravilno osmišljeni programi obuke, uz redovne procjene, analizu incidenata i uključivanje uprave, osiguravaju da organizacija ostane proaktivna u zaštiti od cyber prijetnji. Kroz ovaj pristup, zaposlenici postaju snažnija karika u lancu sigurnosti, smanjujući rizik od ljudskih grešaka i unapređujući ukupnu otpornost organizacije na cyber napade.

13. Sigurnost lanca snabdijevanja

Sigurnost lanca snabdijevanja postaje sve važniji aspekt cyber sigurnosti, s obzirom na to da prijetnje ne dolaze samo iz unutrašnjosti organizacije, već i kroz vanjske partnere i dobavljače. Upravljanje sigurnošću lanca snabdijevanja pomaže u identifikaciji i mitigaciji rizika povezanih s vanjskim entitetima na koje organizacija ovisi.

Koraci implementacije

1. **Razumijevanje i analiza lanca snabdijevanja:** Prvi korak je potpuno razumijevanje lanca snabdijevanja organizacije. Ovo uključuje mapiranje svih vanjskih partnera, dobavljača i drugih trećih strana koje igraju ključnu ulogu u poslovnim operacijama. Razumijevanje svakog segmenta lanca omogućava precizniju identifikaciju potencijalnih sigurnosnih prijetnji i slabih tačaka.
2. **Identifikacija ključnih dobavljača i partnera:** Kreirajte listu svih dobavljača i partnera, te identificirajte one koji predstavljaju najveći rizik po sigurnost organizacije. Ovi dobavljači su obično oni koji imaju pristup kritičnim sistemima, podacima ili poslovnim procesima organizacije. Postavljanje prioriteta omogućava fokusiranje sigurnosnih napora na najkritičnije odnose.
3. **Razvijanje zajedničkog razumijevanja sigurnosnih odgovornosti:** Razvijte zajedničko razumijevanje sa svim dobavljačima i partnerima o sigurnosnim odgovornostima svake strane. Ovi dogovori trebaju biti formalizirani kroz ugovore ili sporazume koji jasno definiraju ko je odgovoran za koji aspekt sigurnosti, uključujući zaštitu podataka, odgovor na incidente, i kontinuitet poslovanja. Ova transparentnost pomaže u osiguravanju da su svi uključeni u lanac snabdijevanja svjesni svojih obaveza i spremni da ih ispune.
4. **Uključivanje partnera u vježbe odgovora na incidente:** Gdje je to prikladno, uključite ključne partnere i dobavljače u vježbe odgovora na incidente. Ove vježbe pomažu u testiranju zajedničke spremnosti na incident, identificiranju potencijalnih slabosti u komunikaciji i koordinaciji, te u osiguravanju da svi partneri znaju svoje uloge i odgovornosti u slučaju stvarnog incidenta.

Zaključak: Sigurnost lanca snabdijevanja zahtijeva sveobuhvatan pristup koji uključuje razumijevanje svakog segmenta lanca, identifikaciju ključnih partnera i razvijanje jasnih sigurnosnih odgovornosti. Kroz uspostavljanje prioriteta, formalizaciju sigurnosnih odgovornosti i redovne vježbe s ključnim partnerima, organizacija može značajno smanjiti rizik od prijetnji koje dolaze putem vanjskih entiteta i osigurati da lanac snabdijevanja ostane siguran i pouzdan.

Reference

Federal Trade Commission (no date), Understanding the NIST cybersecurity framework, https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf

National Cyber Security Centre (no date), Small Business Guide: Cyber Security, https://www.ncsc.gov.uk/collection/small-business-guide

National Cyber Security Centre (no date), 10 Steps to Cyber Security, https://www.ncsc.gov.uk/collection/10-steps

Statista (2024), Concerns about the internet in the Western Balkans in 2023, https://www.statista.com/statistics/1488114/concerns-about-the-internet-in-the-western-balkans/#statisticContainer

Statista (2024), Estimated number of small and medium sized enterprises (SMEs) worldwide from 2000 to 2023, by region, https://www.statista.com/statistics/1261598/global-smes-by-region/

Statista (2024), Number of small and medium-sized enterprises (SMEs) in the European Union from 2008 to 2023, by number of enterprises, https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/

Verizon (no date), Is your front door open and unlocked for cyber criminals? https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches/