NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

REKOMENDACIJOS DĖL ELEKTRONINIO PAŠTO SAUGUMO KONTROLĖS PRIEMONIŲ

RUGPJŪTIS

2025

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.

Turinys

Rekomendacijų tikslas

El. paštas yra viena plačiausiai naudojamų ir efektyviausių komunikacijos priemonių organizacijose. Kasdien visame pasaulyje išsiunčiama ir gaunama daugiau kaip 300 milijardų el. laiškų. El. pašto sprendimai tapo kasdienybe tiek vidiniam darbuotojų bendravimui, tiek išorinei komunikacijai su klientais ir partneriais.

Šiame informaciniame leidinyje apžvelgiamos pagrindinės su el. paštu susijusios grėsmės bei taikytinos saugumo kontrolės priemonės.

Dėl tokio populiarumo bei sąlyginai nesudėtingo išnaudojimo, el. paštas taip pat tapo vienu iš pagrindinių kibernetinių atakų vektoriumi.

1. El. pašto saugumo grėsmės

El. paštu dažniausiai yra vykdomos socialinės inžinerijos atakos. Nors įprastai žmogus yra pagrindinis socialinės inžinerijos atakų taikinys, tačiau vis dažniau atakoms vykdyti yra išnaudojama ir netinkama el. pašto paslaugos sprendimo konfigūracija, neatnaujinta pažeidžiama programinė įranga bei saugumo kontrolės priemonių trūkumai.

Duomenų viliojimas, sukčiavimas (angl. *Phishing*)

Dažniausiai apgaule, apsimetant jums žinomu asmeniu ar įmone, yra siekiama išgauti neviešą informaciją ar prieigą prie informacijos. Įprastai yra gaunami el. laiškai, kuriuose yra prašoma atidaryti kenkėjiškas nuorodas ar atsisiųsti priedus.

Apsimetimas kitu (angl. *Spoofing*)

Taktika, kuomet sukčiai suklastoja el. laiško siuntėjo ar jo domeno informaciją, siekdami apgauti el. laiško gavėją ir jį įtikinti, kad el. laiškas yra siunčiamas iš patikimo šaltinio. Ši apgaulė apima tokias taktikas, kaip:

- **Typosquatting –** domenų registravimas su nežymiomis rašybos klaidomis, imituojant klastojamą domeną, pvz., vietoje nksc.lt yra naudojamas domenas nk5c.lt, t. y. vietoje raidės „s" naudojamas skaičius „5".

- **Subdomeno suklastojimas (angl. Subdomain Spoofing)** – kai užpuolikai sukuria apgaulingus domeno subdomenus, kad imituotų autentiškus domenus, pvz., vietoje nksc.lt sukuriamas „NKSC" domeną imituojantis subdomenas - nksc.fake.lt.

Kenkėjiška programinė įranga (angl. *Malware*)

Gaunami el. laiškai, kuriuose yra prašoma atidaryti kenkėjiškas nuorodas ar atsisiųsti priedus. Juos paspaudus ir (ar) parsisiuntus, auka to nesuprasdama į savo įrenginį įdiegia piktavalio parengtą kenkėjišką programinę įrangą.

Pažeidžiamumų išnaudojimas (angl. Vulnerabilities)

Taktika, kuomet piktavaliai pasinaudoja egzistuojančiomis programinės įrangos saugumo spragomis. Ši grėsmė yra labiausiai aktuali, kuomet el. pašto paslaugos sprendimą, pvz., „Microsoft Exchange“ ar „Postfix“, prižiūrite patys bei laiku neįdiegiate gamintojo atnaujinimų. Piktavaliai gali išnaudoti pažeidžiamos el. pašto paslaugos programinės įrangos saugumo spragas, siekdami vykdyti nuotolinio kodo paleidimą, eskaluoti prieigos teises ar nutekinti duomenis.

2. Taikytinos saugumo kontrolės priemonės

Taikomos saugumo kontrolės priemonės riboja piktavalio galimybes klastoti jūsų el. pašto domeną ar taikyti įprastus socialinės inžinerijos metodus. Toliau šiame tekste yra detalizuotos riziką mažinančios, rekomenduojamos įgyvendinti saugumo kontrolės priemonės[1] :

Saugi autentifikacija

Jungiantis prie el. pašto paskyros naudokite sudėtingus slaptažodžius ir kelių faktorių autentifikavimo priemones (angl. MFA), tokias kaip „*Google Authenticator*“ ar „*MS Authenticator*“. Taip pat naudokite slaptažodžių valdymo įrankius, pvz., „*KeePass*“, kad užtikrintumėte saugų slaptažodžių saugojimą.

El. pašto konfigūracija

Sukonfigūruokite SPF (*Send Policy Framework*), DKIM (*Domain Keys Identified Mail*) ir DMARC (*Domain-based Message Authentication, Reporting, and Conformance*) DNS (*Domain Name System*) įrašus, reikalingus saugiai el. laiškų autentifikacijai atlikti. SPF leidžia nurodyti autorizuotus IP adresus, galinčius siųsti el. laiškus jūsų domeno vardu. DKIM suteikia galimybę el. laiškų gavėjui patikrinti jūsų domeno vardu pasirašytų el. laiškų autentiškumą. DMARC nustato politiką, kaip elgtis su el. laiškais, kurie neatitinka SPF ar DKIM sąlygų, ir siųsti domeno savininkui atitinkamas ataskaitas.

[1] Remiantis ISO/IEC organizacijos informacijos saugumo valdymo sistemos standartu - https://www.iso.org/standard/27001

Mokymai ir simuliacijos

Organizacijos darbuotojams reguliariai renkite informacijos saugumo mokymus socialinės inžinerijos ir el. pašto grėsmių tematika. Mokymams pasitelkite socialinės inžinerijos atakų simuliacijas ir vykdykite reguliarius darbuotojų budrumo patikrinimus. Nemokamus Kibernetinio saugumo kursus bei mokymus darbuotojams ir vadovams teikia ir NKSC (https://www.nksc.lt/mokymai/). Realistiškoms kenkėjiškų el. laiškų simuliacijoms vykdyti galite naudoti ir atvirojo kodo įrankius, tokius kaip „GoPhish“.

Stebėjimas ir filtravimas

Įdiekite tarpinius el. laiško turinio analizės ir filtravimo sprendimus (pvz. SEG (angl. *Secure Email Gateway*)), kurie suteikia galimybes filtruoti el. laiškus, skenuoti prisegtus priedus ar nuorodas ir atitinkamai blokuoti įtartinus el. laiškus bei jų siuntėjus dar prieš laiškams pasiekiant adresatus. Į filtravimo sprendimus įtraukite taisykles, ribojančias el. laiškus su prisegtais potencialiai žalingais failais, pavyzdžiui: .exe, .bat, .msi (rekomenduojamų riboti plėtinių sąrašas pateiktas Priede Nr. 2). Papildomai naudokite apsaugos sistemas (pvz. „*Microsoft Defender for Office 365*“), aptinkančias kenkėjiškus failus ir nuorodas. Stebėkite DMARC politikos veikimo ataskaitas, reguliariai ir pasikeitus el. pašto sprendimui ar paslaugos teikėjui atnaujinkite nustatymus.

3. Bazinė DKIM, SPF ir DMARC konfigūracija

Rekomenduojame naudoti DKIM, SPF ir DMARC saugumo priemones, kurios leistų sumažinti el. pašto paslaugai būdingas grėsmes. Įdiegus ir tinkamai sukonfigūravus šias priemones, jūsų organizacijos el. laiškų adresatai bus tikri, jog gaunami pranešimai yra autentiški, o suklastoti el. laiškai jų nepasiekia. Jūs taip pat būtumėte informuojami apie atvejus, kuomet pasinaudojant jūsų domenu būtų bandoma siųsti suklastotus laiškus.

Bazinės konfigūracijos aprašymuose, kaip pavyzdį naudosime "nksc.lt" domeno pavadinimą.

Domain Keys Identified Mail (DKIM)

DKIM tai el. laiško antraštėje įterptas skaitmeninis parašas, kuris parodo, jog el. laiško turinys yra autentiškas ir pasirašytas jį siunčiančio domeno savininko. El. laišką priimantis el. pašto serveris skaitmeninio parašo autentiškumą gali patikrinti pagal el. laiško siuntėjo domeno DNS įraše pateiktą viešąjį raktą ir jo atributus.

DKIM konfigūravimas

DKIM tai el. laiško antraštėje įterptas skaitmeninis parašas, kuris parodo, jog el. laiško turinys yra autentiškas ir pasirašytas jį siunčiančio domeno savininko. El. laišką priimantis el. pašto serveris skaitmeninio parašo autentiškumą gali patikrinti pagal el. laiško siuntėjo domeno DNS įraše pateiktą viešąjį raktą ir jo atributus.

Prisijunkite prie el. pašto paslaugų teikėjo administratoriaus paskyros. Sukurkite DKIM raktų porą[2]. Dauguma el. pašto paslaugų teikėjų, tokių kaip „*Microsoft*“ arba „*Google*“, siūlo integruotą DKIM rakto kūrimo įrankį.

[2]Pastaba - naudokite sudėtingesnį negu 2048-bit šifravimo algoritmą

Sugeneravus raktų porą, bus sugeneruotas viešojo rakto įrašas, kurį reikės įvesti DNS paslaugų teikėjo administratoriaus paskyroje kaip „TXT" tipo įrašą[3]. „TXT“ tipo įrašas yra naudojamas tiesioginiam viešojo rakto įvedimui į DNS įrašus, tačiau, jei DKIM viešasis raktas dažnai kinta ar jį valdo el. pašto paslaugų teikėjas, tuomet, siekiant išvengti nuolatinio jo atnaujinimo, vietoje „TXT“ įrašo gali būti naudojamas „CNAME“ tipo įrašas. Jis DNS įrašo interesantus nukreipia į paslaugų teikėjo valdomą adresą, kuriame yra pateikiamas aktualus DKIM viešasis raktas:

Google paslaugų teikėjo atveju:

„TXT" įrašo pavadinimas:
google._domainkey.nksc.lt

„TXT" įrašo reikšmė:
v=DKIM1;
k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAquku+knisZ+hErO8UkGTE5wp/Lpn+c43Ca9prRJVBkdHHvYOpxHo2hUo0Z2HenrT96OlC1a+vfJGSi6LEemmOtrKOMeHyvAwd2kZlrGL0/PHoEY8+LEJ02gHVpXUg5R0efD3VFoYj0P9g94fJ35eq3YlLlindAVNZsh6fwfTXgqYhG2NWRGlSoimbtyUWlrKattIVE5u6oqBpX8A3+lJhIN0wM7eGjeXTiLzKSp6b4LthQRTW8DIACyFM1lLpdddha891KfwedMY7408F2zCSIRbIEpcnnM7gScXlnuYx8iCTsISvIBQ4h3GnK7VaMNowxzDTnw4MMMt5EY0L2N64QIDAQAB

Microsoft paslaugų teikėjo atveju:

„CNAME" įrašo pavadinimas:
selector1._domainkey.nksc.lt

„CNAME" įrašo reikšmė:
selector1-nksc-lt._domainkey.nksc.onmicrosoft.com

[3] Įvedus DKIM įrašą būtinai aktyvuokite DKIM autentifikaciją paslaugų tiekėjo administratoriaus paskyroje.

Sender Policy Framework (SPF)

SPF tai domeno DNS įrašas, kuriame nurodoma, kuriems IP adresams yra leidžiama siųsti el. laiškus domeno vardu. Jeigu yra naudojamas el. pašto paslaugų teikėjas, pavyzdžiui, *Google* ar *Microsoft*, tuomet turi būti nurodytas to el. pašto paslaugos teikėjo SPF politiką nustatantis IP adresas ar domenas.

SPF konfigūravimas

Pagrindinės reikšmės[4]:

v=spf1	Nurodo, kad tai *SPF* tipo įrašas.
a	Nurodo, kad domeno *DNS* "A" tipo įraše nurodytas IP adresas yra autorizuotas siųsti el. laiškus domeno vardu.
mx	Nurodo, kad domeno *DNS* "MX" tipo įraše nurodytas domenas yra el. pašto serveris, autorizuotas priimti el. laiškus domeno vardu.
include: *[domenas/ip adresas]*	Nurodo domeną ir / arba IP adresą, kuriame aprašyti domenai / IP adresai, galintys siųsti el. laiškus domeno vardu.
redirect= *[domenas]*	Tai modifikatorius, kuris nukreipia *SPF* įrašą naudoti iš kito domeno. Naudojant ***redirect*** modifikatorių *SPF* įraše negali būti aprašyta **all** reikšmė. Šį modifikatorių reikėtų tik įsitikinus, kad *SPF* įrašas kitame domene yra tinkamai sukonfigūruotas, priešingu atveju visas SPF įrašas nebeveikia.
-all **~all** **+all** **?all**	**-all** nurodo, kad *SPF* įraše nenurodytiems IP adresams ir domenams yra uždrausta siųsti el. laiškus domeno vardu (tokie laiškai bus ignoruojami). Tai yra saugiausia parinktis. **~all** nurodo, kad iš neautorizuotų serverių ar IP adresų gauti el. laiškai turi būti traktuojami kaip šlamštas ir nukeliauti į šlamšto katalogą (laiškai bus gaunami, tačiau bus užskaitomi kaip šlamštas). **+all** nurodo, kad bet kuris serveris gali siųsti el. laiškus domeno vardu (laiškai bus gaunami ir nebus užskaityti kaip šlamštas). **?all** nurodo, kad atmetimo politika nesukonfigūruota (laiškas bus priimtas visais atvejais).

[4] Daugiau informacijos apie SPF įrašo nustatymą ir mechanizmus galima rasti - IETF. (2014 m. 04). Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. Nuskaityta iš ietf.org: https://datatracker.ietf.org/doc/html/rfc7208

Prisijunkite prie DNS paslaugų teikėjo administratoriaus konsolės ir sukurkite „TXT" tipo įrašą, kurio reikšmės būtų:

	Google atveju	**Microsoft atveju**
„*TXT*" įrašo pavadinimas	@	@
„*TXT*" įrašo vertė (jeigu naudojate tik el. pašto paslaugų teikėjų serverius)	v=spf1 include:_spf.google.com -all	v=spf1 include:spf.protection.outlook.com -all
„*TXT*" įrašo vertė (jeigu papildomai naudojate ir savo el. pašto paslaugos serverį bei norite jam teikti prioritetą)	v=spf1 a mx include:_spf.google.com -all	v=spf1 a mx include:spf.protection.outlook.com -all

Domain-based Message Authentication, Reporting and Conformance (DMARC)

DMARC konfigūravimas

Reikšmės[5]:

rua	El. pašto adresas, kuriam bus siunčiamos apibendrintos ataskaitos apie tai, kas ir kiek el. laiškų siuntė, kurie el. laiškai neatitiko nustatytų *SPF* ir / arba *DKIM* sąlygų.
ruf	El. pašto adresas, kuriam bus siunčiami pranešimai apie serverių IP adresus, kurie siuntė el. laiškus, neatitinkančius nustatytų *SPF* ir / arba *DKIM* sąlygų.
ri	Nurodo, kas kiek sekundžių yra išsiunčiamos rua ataskaitos. Numatytoji reikšmė yra 86400 sekundžių (1 diena).
fo	Ataskaitų, kurios siunčiamos ruf mechanizme nurodytam el. pašto adresui, tipas: fo=0: ataskaita siunčiama, kai el. laiškas neatitinka *SPF* ir *DKIM* sąlygų. fo=1: ataskaita siunčiama, kai el. laiškas neatitinka *SPF* arba *DKIM* sąlygų. fo=d: *DKIM* trikdžių ataskaita siunčiama nepaisant to, ar el. laiškas atitinka nustatytas *DKIM* sąlygas. fo=s: *SPF* trikdžių ataskaita siunčiama nepaisant to, ar el. laiškas atitinka nustatytas *SPF* sąlygas.
pct	Nurodo, kokiam procentui (1-100) laiškų yra taikoma *DMARC* politika.

Prisijunkite prie DNS paslaugų teikėjo administratoriaus konsolės ir sukurkite „TXT" tipo įrašą, kurio reikšmės būtų:

„*TXT*" įrašo pavadinimas	@

„*TXT*" įrašo vertė	v=DMARC1;
	p=reject;
	rua=mailto:reports@nksc.lt;
	ruf=mailto:forensics@nksc.lt;
	ri=86400;
	fo=1;
	pct=100

[5] Daugiau informacijos apie DMARC politikos nustatymą ir mechanizmus galima rasti - IETF. (2015 m. 2 5 d.). DMARC Technical Specification. Nuskaityta iš DMARC Technical Specification: https://datatracker.ietf.org/doc/html/rfc7489

Remiantis gerąja praktika, įgyvendinant DMARC politiką, yra rekomenduojama taikyti laipsniškai griežtėjančią politiką. Pradėkite nuo politikos „p=none“, kad surinktumėte pirminius duomenis, tuomet palaipsniui didinkite sąlygų griežtumą iki "p=quarantine" ir galiausiai "p=reject". Reguliariai stebėkite gaunamas DMARC ataskaitas, kad nustatytumėte tinkamiausius SPF ir DKIM įrašų mechanizmus bei identifikuotumėte neteisėtus el. laiškų siuntimo šaltinius.

4. Naudingi įrankiai ir mokymai

Pasitikrinimo klausimynas

Kviečiame įsivertinti šiuo metu organizacijoje įgyvendintas el. pašto saugumo kontrolės priemones bei nustatyti, kurias šiame informaciniame leidinyje apžvelgtas rekomendacijas dar reikėtų įgyvendinti. El. pašto saugumo kontrolių priemonių sąrašą rasite **Priede Nr. 1.**

Kibernetinio saugumo kursai darbuotojų budrumui stiprinti

NKSC viešai prieinamoje mokymų platformoje **https://www.nksc.lt/mokymai/** teikia darbuotojams ir vadovams nemokamus kibernetinio saugumo kursus: „Kibernetinė higiena darbe“, „Kibernetinė sauga vadovams”.

Papildomi įrankiai pasitikrinimui

Po atliktos SPF, DKIM ir DMARC įrašų konfigūracijos rekomenduojama pasitikrinti domeno DNS įrašų tinkamumą. Patikrinti iš išorės galima, naudojant šiuos įrankius:

https://sauguspastas.nksc.lt

NKSC adaptuotas DKIM, SPF ir DMARC įrašus tikrinantis įrankis padės identifikuoti DNS įrašuose esančias konfigūracijos klaidas bei pateiks siūlymus, kuriuos mechanizmus reikėtų taisyti.

https://mxtoolbox.com

„MXToolBox" MX įrašų, DNS , juodojo sąrašo ir SMTP (Simple Mail Transfer Protocol) diagnostikos įrankis

Priedas nr.1: El. pašto saugumo įsivertinimo kontrolinis klausimynas

Saugi autentifikacija ir prieigos kontrolė

- [ ] 1. Ar el. pašto paskyroms naudojami stiprūs slaptažodžiai?
- [ ] 2. Ar visiems naudotojams įjungta kelių faktorių autentifikacija (MFA)?
- [ ] 3. Ar naudojami slaptažodžių valdymo įrankiai?

El. pašto paslaugos ir DNS konfigūracija (SPF, DKIM, DMARC)

- [ ] 4. Ar sukonfigūruotas DKIM įrašas tuo tikslu, kad laiškai būtų pasirašomi ir apsaugomi nuo klastojimo?
- [ ] 5. Ar sukonfigūruotas SPF įrašas, nurodantis autorizuotus IP adresus, galinčius siųsti el. laiškus jūsų domeno vardu?
- [ ] 6. Jei laiškai siunčiami iš kelių paslaugų teikėjų, ar visi jie įtraukti į SPF (include)?
- [ ] 7. Ar SPF įrašas naudoja -all (griežtą atmetimą), kai visi teisėti siuntėjai patvirtinti?
- [ ] 8. Ar tinkamai sukonfigūruoti MX įrašai, rodantys į patikimus pašto serverius?
- [ ] 9. Ar ištestuota DMARC politika su pradine p=none reikšme?
- [ ] 10. Ar nustatyta DMARC politika su p=quarantine arba p=reject reikšmėmis?
- [ ] 11. Ar gaunamos ir reguliariai stebimos DMARC ataskaitos bei tikrinami el. laiškų siuntimo šaltiniai?

Apsauga nuo kenkėjiškų laiškų

- [ ] 12. Ar įdiegtas ir sukonfigūruotas tarpinis el. pašto saugumo sprendimas (Secure Email Gateway, SEG), filtruojantis pavojingus el. laiškus?
- [ ] 13. Ar naudojamas apsaugos įrankis ar antivirusinė programa, pvz., Microsoft Defender for Office 365 arba panašūs?
- [ ] 14. Ar uždraustas pavojingų failų plėtinių gavimas el. paštu (žr. į Priedą Nr. 2)?

Saugumo testavimas ir darbuotojų mokymai

- [ ] 15. Ar organizacijoje reguliariai vykdomos sukčiavimo (phishing) atakų simuliacijos?
- [ ] 16. Ar darbuotojams yra periodiškai primenama, kaip atpažinti el. pašto grėsmes (phishing, spoofing, malware)?
- [ ] 17. Ar organizacijos darbuotojai dalyvavo NKSC organizuojamuose kibernetinio saugumo mokymuose (https://www.nksc.lt/mokymai/)?
- [ ] 18. Ar ištestuota el. pašto paslaugos ir DNS konfigūracija, naudojant NKSC saugaus pašto įrankį (https://sauguspastas.nksc.lt)?

Pažeidžiamumų valdymas (jeigu patys talpinate ir valdote el. pašto paslaugos sprendimą)

- [ ] 19. Ar el. pašto paslaugos serverių programinė įranga reguliariai atnaujinama?
- [ ] 20. Ar el. pašto paslaugos infrastruktūroje yra atliekami periodiniai pažeidžiamumų vertinimai?

Priedas nr.2: kenksmingi failai

Vykdomieji failai – didžiausia grėsmė

Laiškus, turinčius prisegtų šio tipo failų, rekomenduojama blokuoti:

.exe – Windows vykdomasis failas;

.bat – Batch vykdomo kodo rinkinio failas;

.cmd – Windows komandinės eilutės vykdomasis kodo rinkinys;

.msi – Microsoft pritaikytų bibliotekų rinkinys diegimui;

.vbs, .js, .jse, .wsf – kodo rinkiniai, galintys inicijuoti kenkėjiško kodo vykdymą;

.ps1, .psm1, .psd1 – PowerShell vykdomojo kodo rinkiniai;

.sh, .bash – Linux/Mac shell vykdomojo kodo rinkiniai.

Archyvai ir suspausti failai – padidintas dėmesys

Rekomenduojama tikrinti ir, esant įtarimams, blokuoti:

.zip, .rar, .7z – ypač tada, kai apsaugoti slaptažodžiu;

.iso, .img – galintis slėpti kenkėjišką programinę įrangą;

.tar, .gz – retai naudojamas, tačiau potencialiai pavojingas;

.ace – pasenęs archyvavimo formatas, dažnai pasitelkiamas kibernetinėse atakose.

Dokumentai su makro komandomis – padidintas dėmesys

Riboti ir, esant įtarimams, blokuoti:

.docm, .xlsm, .pptm – Microsoft Office dokumentai su įterptomis makrokomandomis;

.rtf – dažnai naudojamas naujoms atakoms vykdyti (angl. zero-day).

Kiti pavojingi failų tipai
Rekomenduojama blokuoti:

.lnk – Windows nuorodos, dažnai naudojamos kibernetiniuose išpuoliuose;

.htm, .html – HTML failai, dažnai naudojami "phishing" atakoms ir kenkėjiškiems kodo rinkiniams vykdyti;

.scr – ekrano užsklandos, galinčios slėpti kenkėjišką kodą;

.cpl – valdymo skydo failai, galintys vykdyti kenkėjišką kodą;

.jar – Java archyvai, galintys išnaudoti pažeidžiamumus;

.rdp – nuotolinio prisijungimo failai, naudojami prisijungti prie nutolusių galinių įrenginių;

.reg – Windows operacinės sistemos registro failai, galintys pakeisti esamus nustatymus;

.scf – Windows Explorer valdymo failai.

ELEKTRONINIO PAŠTO
SAUGUMO KONTROLĖS PRIEMONĖS

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

El. paštas yra viena pagrindinių ir plačiausiai naudojamų komunikacijos priemonių oranizacijose, tačiau dėl savo populiarumo jis tapo ir dažnu kibernetinių atakų taikiniu.

GRĖSMĖS

El. paštas dažnai tampa socialinės inžinerijos atakų taikiniu, pasinaudojant tiek žmonių patiklumu, tiek netinkamai sukonfigūruotomis sistemomis.

Duomenų viliojimas
(angl. Phishing)

Apgaulingi laiškai, apsimetant pažįstamu siuntėju, siekia išvilioti prisijungimus ar kitą jautrią informaciją.

Apsimetimas kitu asmeniu
(angl. Spoofing)

Suklastotas siuntėjo vardas ar domenas, siekiant apsimesti patikimu šaltiniu.

Kenkėjiška programinė įranga
(angl. Malware)

Laiškai su kenkėjiškomis nuorodomis ar priedais, kurie įdiegia žalingą programinę įrangą.

Pažeidžiamumų išnaudojimas
(angl. Vulnerabilities)

Atakos, išnaudojančios el. pašto sistemos saugumo spragas ar neatnaujintą programinę įrangą.

SAUGUMO PRIEMONĖS

Saugumo kontrolės priemonės, kurios sumažina riziką tapti el. pašto apgavysčių taikiniu.

Saugi autentifikacija

Naudokite stiprius slaptažodžius, kelių veiksnių autentifikavimą (MFA) ir slaptažodžių valdymo įrankius, pvz., „KeePass“.

El. pašto konfigūracija

Sukonfigūruokite SPF, DKIM ir DMARC įrašus, kurie padeda apsaugoti el. paštą nuo klastojimo ir neteisėto panaudojimo.

Mokymai ir simuliacijos

Reguliariai organizuokite darbuotojų mokymus ir vykdyti socialinės inžinerijos atakų simuliacijas.

Stebėjimas ir filtravimas

Naudokite el. laiškų filtravimo, antivirusines ir stebėsenos priemones, taip pat riboti pavojingų priedų plėtinius.

SPF
Sender Policy Framework

SPF yra domeno DNS įrašas, kuris nurodo, kokie IP adresai gali siųsti el. laiškus šio domeno vardu. Naudojant el. pašto paslaugų teikėjus (pvz., Google, Microsoft), būtina įtraukti jų SPF nustatymus.

DKIM
Domain Keys Identified Mail

DKIM tai el. laiško antraštėje esantis skaitmeninis parašas, patvirtinantis, kad laiškas yra autentiškas ir pasirašytas siuntėjo domeno savininko. Jo tikrumą gavėjo serveris patikrina pagal DNS įraše nurodytą viešąjį raktą.

DMARC
Domain-based Message Authentication, Reporting and Conformance

DMARC yra domeno DNS įrašas, nustatantis, kaip gavėjo serveris turi vertinti siuntėjo duomenis (IP adresą, skaitmeninį parašą) ir ką daryti, jei laiškas neatitinka SPF ar DKIM taisyklių.

NAUDINGI ĮRANKIAI IR MOKYMAI

Patikrinkite savo el. pašto saugumą

sauguspastas.nksc.lt – patikrinkite SPF, DKIM ir DMARC įrašus, raskite klaidas ir gaukite pataisymų rekomendacijas.

Stiprinkite kibernetinio saugumo žinias

nksc.lt/mokymai – nemokami NKSC kursai organizacijų darbuotojams ir vadovams.

Įsivertinkite el.pašto saugumą

Leidinyje rasite priedus su kontroliniais klausimynais, padėsiančiais įsivertinti patikrinti el. pašto saugumą.

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.