ME/PSO

DORACAK

Doracak për sigurinë e postës elektronike

Mbrojtja nga phishing-u, bashkëngjitjet keqdashëse dhe mashtrimet përmes postës elektronike

Material shoqërues për trajnimin:
„Siguria e postës elektronike“

Dokument nr. MEPSO-PRI-MAIL-002 · Klasifikimi: Përdorim i brendshëm
Sektori i sigurisë informatike dhe kibernetike · MEPSO SHA Shkup

Përmbajtja

1. Hyrje

Posta elektronike është mjeti më i përdorur i komunikimit afarist — dhe pikërisht për këtë, pika më e shpeshtë e hyrjes për sulmet kibernetike. Mbi 90% e sulmeve të suksesshme fillojnë me një email.

Ky doracak do t’ju ndihmojë t’i njihni kërcënimet që vijnë përmes postës elektronike dhe të zhvilloni zakone që ju mbrojnë ju dhe organizatën. Nuk do t’ju bëjë ekspert teknik — do t’ju bëjë përdorues të vëmendshëm dhe të informuar, që është më e rëndësishme.

Çdo ditë merrni dhjetëra mesazhe. Ndërmjet tyre, herë pas here, fshihet ndonjë që është dizajnuar për t’ju mashtruar, për të vjedhur të dhëna ose për të instaluar softuer keqdashës. Ndryshimi ndërmjet një sistemi të sigurt dhe një sistemi të komprometuar shpesh është një klik i vetëm.

> **Mendimi kyç.** Sistemet më të sofistikuara të sigurisë mund të anashkalohen me një email të menduar mirë që e mashtron njeriun të klikojë. Ju jeni mbrojtja më e rëndësishme.

2. Pse posta elektronike është cak i sulmeve

Sulmuesit e pëlqejnë postën elektronike për disa arsye:

- **Shtrirja** — një mesazh mund t’u dërgohet mijëra njerëzve njëkohësisht;
- **Besimi** — njerëzit janë mësuar t’i hapin mesazhet dhe të klikojnë në linqe;
- **Imitimi i lehtë** — është relativisht e lehtë të shtiresh se je dikush tjetër;
- **Qasja e drejtpërdrejtë** — emaili të çon drejtpërdrejt te përdoruesi, duke anashkaluar shumë mbrojtje teknike;
- **Faktori njerëzor** — shfrytëzimi i kureshtjes, frikës ose urgjencës.

2.1 Çfarë duan të arrijnë

Qëllimi	Metoda
Vjedhja e fjalëkalimeve	Faqe të rreme për kyçje
Instalimi i softuerit keqdashës	Bashkëngjitje të infektuara
Mashtrimi financiar	Fatura të rreme, kërkesa për transfer
Vjedhja e të dhënave	Manipulim për të zbuluar informacione
Qasja në sisteme	Komprometimi i një llogarie përdoruesi

3. Anatomia e një kërcënimi me email

Për ta njohur një mesazh të dyshimtë, është e rëndësishme t’i dini elementet që sulmuesit i shfrytëzojnë.

3.1 Adresa e dërguesit

Elementi më i rëndësishëm për kontroll. Sulmuesit përdorin adresa që ngjajnë me ato legjitime, me dallime të vogla që anashkalohen lehtë — një shkronjë e zëvendësuar, një shenjë shtesë, një domen i ngjashëm.

> **Kini kujdes.** Një adresë si mepso-it.com nuk është e njëjtë me mepso.com.mk. Gjithmonë kontrolloni domenin e plotë, jo vetëm emrin që shfaqet.

3.2 Titulli (Subject)

Titujt janë të dizajnuar për të provokuar reagim urgjent: „Urgjente“, „Llogaria juaj është bllokuar“, „Paralajmërimi i fundit“. Urgjenca është taktikë që të mos mendoni qetësisht.

3.3 Trupi i mesazhit

Vëreni përshëndetjet gjenerike („I nderuar përdorues“ në vend të emrit tuaj), gabimet gramatikore, tonin e pazakontë dhe kërkesat për të bërë diçka shpejt.

3.4 Linqet dhe bashkëngjitjet

Këtu fshihet rreziku i vërtetë. Linqet çojnë në faqe të rreme, kurse bashkëngjitjet përmbajnë kod keqdashës.

4. Phishing — njohja dhe mbrojtja

Phishing-u është lloji më i shpeshtë i sulmit përmes emailit. Sulmuesi shtiret se është institucion i besueshëm për t’ju shtyrë të zbuloni të dhëna të ndjeshme.

4.1 Llojet e phishing-ut

Lloji	Përshkrimi
Phishing masiv	I njëjti mesazh dërguar mijëra marrësve
Spear phishing	I drejtuar te një person konkret, me detaje personale
Whaling	I drejtuar te udhëheqësit dhe funksionet e larta
Clone phishing	Kopje e një mesazhi legjitim me linqe të ndryshuara

4.2 Flamujt e kuq

- ✓ Urgjenca dhe presioni për veprim të shpejtë
- ✓ Kërkesa për fjalëkalim, PIN ose të dhëna personale
- ✓ Përshëndetje gjenerike në vend të emrit tuaj
- ✓ Gabime gramatikore dhe drejtshkrimore
- ✓ Adresë e dyshimtë e dërguesit
- ✓ Ofertë tepër e mirë (shpërblime, fitime)
- ✓ Linqe që nuk përputhen me tekstin e shfaqur

Shembull phishing-u:
„I nderuar përdorues, kemi vërejtur aktivitet të pazakontë në llogarinë tuaj. Për ta konfirmuar, klikoni këtu dhe vendosni të dhënat tuaja brenda 2 orëve, përndryshe llogaria do të bllokohet përgjithmonë.“
Shenjat: përshëndetje gjenerike, urgjencë, kërkesë për të dhëna, presion.

4.3 Si të mbroheni

- ✓ Ndaluni para se të reagoni ndaj kërkesave urgjente
- ✓ Kontrolloni me kujdes adresën e dërguesit
- ✓ Kaloni me maus mbi link për ta parë adresën e vërtetë
- ✓ Shkruajini adresat në shfletues me dorë, në vend që të ndiqni linqe
- ✓ Kurrë mos vendosni fjalëkalim në një faqe ku keni arritur përmes linku
- ✓ Në rast dyshimi, konfirmoni përmes telefonit zyrtar

5. Bashkëngjitjet keqdashëse

Bashkëngjitjet janë mënyrë e shpeshtë e përhapjes së softuerit keqdashës. Hapja e një bashkëngjitjeje të infektuar mund të instalojë virus, ransomware ose program spiunimi.

5.1 Llojet e rrezikshme të skedarëve

Lloji	Rreziku
.exe, .scr, .bat	Programe të ekzekutueshme — rrezik i lartë
.zip, .rar	Skedarë të kompresuar që e fshehin përmbajtjen
.docm, .xlsm	Dokumente me makro që ekzekutojnë kod
.js, .vbs	Skripte që ekzekutojnë komanda

Rregull. Mos hapni bashkëngjitje nga dërgues të panjohur. Edhe nga të njohurit — nëse nuk e prisnit skedarin, konfirmoni përmes një kanali tjetër para se ta hapni.

5.2 Makrot në dokumente

Kur hapni një dokument që kërkon „Aktivizo makrot“ — ndaluni. Dokumentet legjitime rrallë e kërkojnë këtë. Aktivizimi i makrove mund të ekzekutojë kod keqdashës.

6. Linqet e rrezikshme

Linqet maskohen që të duken të sigurta, por çojnë në faqe të rrezikshme.

6.1 Si ta kontrolloni një link

- ✓ Kaloni me maus mbi link (pa klikuar) — adresa e vërtetë shfaqet poshtë

- ✓ Kontrolloni a përputhet domeni me atë që pritet
- ✓ Kini kujdes me linqet e shkurtuara që e fshehin destinacionin e vërtetë
- ✓ Nëse linku kërkon të vendosni të dhëna, jini veçanërisht të kujdesshëm

> **Këshillë.** Nëse merrni mesazh nga një bankë ose institucion me link, mos klikoni. Në vend të kësaj, hapni një dritare të re dhe shkruajeni me dorë adresën zyrtare. Kështu jeni të sigurt se jeni në faqen e vërtetë.

7. Spami dhe posta e padëshiruar

Spami është postë masive e padëshiruar. Edhe pse shpesh është vetëm i bëzdisshëm, mund të përmbajë edhe kërcënime.

- ✓ Mos iu përgjigjni spamit — kjo konfirmon se adresa është aktive
- ✓ Mos klikoni „çregjistrohu“ në mesazhe të dyshimta — mund të jetë kurth
- ✓ Shënojeni spamin për ta përmirësuar filtrimin
- ✓ Mos e publikoni adresën tuaj afariste në vende publike pa nevojë

8. Kompromet imi i email-it afarist (BEC)

Business Email Compromise është sulm i sofistikuar ku sulmuesi shtiret se është udhëheqës ose partner për të nxitur një transaksion financiar ose zbulimin e të dhënave.

8.1 Skenari tipik

Merrni një mesazh që duket se është nga një drejtor, me kërkesë urgjente për transfer të mjeteve ose dërgim të dhënash konfidenciale. Toni është autoritar dhe urgjent.

> **Kujdes.** Çdo kërkesë e pazakontë për transfer parash ose të dhëna konfidenciale, edhe nëse duket se vjen nga një udhëheqës, duhet të konfirmohet përmes një telefonate të drejtpërdrejtë ose komunikimi personal.

8.2 Mbrojtja

- ✓ Konfirmojini kërkesat e pazakonta financiare përmes një kanali të dytë
- ✓ Kini kujdes ndaj ndryshimeve në detajet e pagesës
- ✓ Mos u mbështetni vetëm në email për transaksione të rëndësishme
- ✓ Raportoni menjëherë kërkesat e dyshimta

9. Enkriptimi dhe privatësia

Informacionet e ndjeshme të dërguara me postë elektronike duhet të mbrohen.

- ✓ Mos dërgoni fjalëkalime ose të dhëna konfidenciale në tekst të hapur

- ✓ Përdorni enkriptim për bashkëngjitjet e ndjeshme ku është i disponueshëm
- ✓ Kini kujdes se kujt i dërgoni — kontrollojini dy herë marrësit
- ✓ Shmangni „Përgjigju të gjithëve“ përveç kur është vërtet e nevojshme

Gabim i shpeshtë. Dërgimi aksidental i një informacioni konfidencial te marrësi i gabuar është incident i shpeshtë. Gjithmonë kontrollojeni adresën e marrësit para se të shtypni „Dërgo“, sidomos kur plotësimi automatik sugjeron një adresë.

10. Zakone të mira në përdorimin e përditshëm

- ✓ Shqyrtojini mesazhet me kujdes para se të reagoni
- ✓ Kontrollojini adresat e dërguesve
- ✓ Mos klikoni në linqe ose bashkëngjitje në rastin më të vogël të dyshimit
- ✓ Përdorni fjalëkalim të fortë dhe unik për postën elektronike
- ✓ Aktivizoni autentifikimin me dy faktorë
- ✓ Çkyçuni nga posta elektronike në pajisjet e përbashkëta
- ✓ Raportoni mesazhet e dyshimta

11. Çfarë të bëni në rast incidenti

Nëse keni klikuar në një link të dyshimtë, keni hapur një bashkëngjitje ose keni vendosur të dhëna diku ku nuk duhej:

1. Mos u panikosni — reagimi i shpejtë është kyç
2. Ndërprisni lidhjen me internetin nëse dyshoni për softuer keqdashës
3. Ndryshojini menjëherë fjalëkalimet që i keni vendosur
4. Raportoni te Sektori i sigurisë informatike
5. Mos e fshini mesazhin — mund të shërbejë për analizë

Mos kini turp të raportoni. Secili mund të gabojë. Raportimi i shpejtë i mundëson ekipit të sigurisë të reagojë dhe ta kufizojë dëmin. Heshtja vetëm e përkeqëson problemin.

12. Skenarë praktikë

Skenari 1: Mesazh urgjent nga „drejtori“

Merrni një email gjoja nga drejtori i përgjithshëm, me kërkesë urgjente të paguani një faturë në një llogari të re, „sepse është në mbledhje dhe nuk mund të përgjigjet“.

Reagimi i drejtë: Nuk veproni menjëherë. Konfirmoni drejtpërdrejt me drejtorin ose përmes kanalit zyrtar. Urgjenca dhe pamundësia për verifikim janë shenja klasike të mashtrimit BEC.

Skenari 2: Faturë e përcjellë

Një koleg ju përcjell një faturë për pagesë me bashkëngjitje. Bashkëngjitja kërkon të aktivizoni makrot për ta parë përmbajtjen.

Reagimi i drejtë: Nuk aktivizoni makro. Kontrolloni me kolegun a e ka dërguar vërtet dhe a priteshin makro. Faturat legjitime nuk kërkojnë makro.

Skenari 3: Njoftim për pako

Merrni një mesazh se keni një pako të padorëzuar dhe duhet të klikoni një link për ta paguar dërgesën.

Reagimi i drejtë: Nuk klikoni. Nëse prisni pako, shkoni drejtpërdrejt në faqen zyrtare të shërbimit korrier. Njoftimet e rreme për pako janë shumë të shpeshta.

13. Pyetjet më të shpeshta

Si ta di a është e rreme adresa e dërguesit?

Kontrolloni me kujdes domenin e plotë, jo vetëm emrin e shfaqur. Kërkoni dallime të vogla — shkronja të zëvendësuara, shenja shtesë, domen të ngjashëm por jo identik.

A është e sigurt të hap një bashkëngjitje PDF?

PDF-të në përgjithësi janë më të sigurta se skedarët e ekzekutueshëm, por edhe ato mund të përmbajnë kod keqdashës. Hapini vetëm nga dërgues të besueshëm që i keni pritur.

Po nëse klikova një link, por nuk vendosa asgjë?

Raportoni gjithësesi. Disa linqe mund të instalojnë softuer keqdashës vetëm me hapjen. Ekipi i sigurisë do të vlerësojë a ka rrezik.

A më mbron plotësisht filtri i spamit?

Jo. Filtrat kapin shumë, por jo gjithçka. Sulmet më të sofistikuara shpesh kalojnë. Vëmendja juaj mbetet e domosdoshme.

A mund të më vidhet fjalëkalimi vetëm me hapjen e një mesazhi?

Rrallë, por është e mundur me disa sulme të avancuara. Prandaj mos hapni mesazhe nga dërgues të panjohur dhe kurrë mos vendosni të dhëna përmes një linku nga një mesazh.

14. Fjalorthi dhe lista e kontrollit

Termi	Kuptimi
Phishing	Mashtrim përmes mesazheve të rreme për vjedhje të dhënash
Spear phishing	Phishing i drejtuar te një person konkret
BEC	Kompromet im i email-it afarist — mashtrim me identitet të rremë
Bashkëngjitje keqdashëse	Skedar që përmban kod të dëmshëm
Makro	Komandë e automatizuar në dokument, mund të keqpërdoret
Spam	Postë masive e padëshiruar
Domen	Pjesa e adresës pas shenjës @

Lista e shpejtë e kontrollit para çdo kliku

- ✓ A e njoh dhe a e pres adresën e dërguesit?
- ✓ A krijon titulli urgjencë artificiale?
- ✓ A kërkon mesazhi fjalëkalim ose të dhëna personale?
- ✓ Ku çon vërtet linku (kontrolluar me maus)?
- ✓ A e prisja këtë bashkëngjitje?
- ✓ Në rast dyshimi — a raportova në vend që të klikoja?

Roli i postës elektronike në punën e MEPSO-s

Si operator i infrastrukturës kritike, MEPSO ka përgjegjësi të shtuar për mbrojtjen e komunikimit. Posta elektronike shpesh përmban informacione të ndjeshme operative dhe afariste, kompromet imi i të cilave mund të ketë pasoja përtej vetë organizatës.

Masa shtesë për infrastrukturën kritike

- ✓ Të dhënat operative kurrë nuk dërgohen përmes kanaleve të pambrojtura
- ✓ Komunikimi me partnerët e jashtëm i nënshtrohet verifikimit shtesë
- ✓ Qasja në email-in afarist nga pajisjet personale kontrollohet
- ✓ Rregullisht kryhen simulime phishing-u për ngritjen e vetëdijes

> **Përgjegjësi e përbashkët.** Siguria e postës elektronike nuk është vetëm detyrë e Sektorit të TI-së. Çdo punonjës që punon me email është pjesë e sistemit mbrojtës të organizatës. Zakonet tuaja ndikojnë drejtpërdrejt në sigurinë e tërë infrastrukturës.

Trajnimi periodik

Kërcënimet ndryshojnë vazhdimisht dhe bëhen më komplekse. Prandaj është e rëndësishme t’i freskoni rregullisht njohuritë përmes trajnimeve dhe të qëndroni të informuar për metodat e reja të mashtrimit. Ky doracak është pjesë e asaj edukate të vazhdueshme.

15. Përfundim

Posta elektronike do të mbetet pjesë qendrore e punës — dhe cak qendror i sulmeve. Vëmendja juaj është mbrojtja më e mirë. Çdo mesazh që e kontrolloni me kujdes, çdo link i dyshimtë që nuk e klikoni, çdo raportim — e gjithë kjo e ndërton sigurinë e MEPSO-s.

> **Mbani mend.** Kur jeni në dilemë, ndaluni dhe pyesni. Një minutë kujdesi mund të parandalojë një incident të madh.

MEPSO SHA Shkup — Operatori i sistemit të transmetimit të energjisë elektrike të Maqedonisë së Veriut
Dokument nr. MEPSO-PRI-MAIL-002 · Klasifikimi: Përdorim i brendshëm
Ky doracak është pronë e MEPSO SHA dhe është i dedikuar për trajnim dhe përdorim të brendshëm.