

ME/PSO

DORACAK

Doracak për sigurinë kibernetike

Vetëdija, njohja e kërcënimeve dhe mbrojtja në botën digjitale

Material shoqërues për trajnimin:
„Ngritja e vetëdijes për sigurinë kibernetike”

Përmbajtja

1. Hyrje
2. Çfarë është siguria kibernetike
3. Peizazhi i kërcënimeve moderne
4. Softueri keqdashës
5. Ransomware — kyçja e të dhënave për shpërblim
6. Inxhinieria sociale
7. Siguria e fjalëkalimeve dhe e llogarive
8. Shfletim i sigurt në internet
9. Pajisjet mobile dhe siguria
10. Siguria në rrjetet publike
11. Mbrojtja e privatësisë
12. Kopjet rezervë dhe rikuperimi
13. Skenarë praktikë
14. Pyetjet më të shpeshta
15. Fjalorthi dhe lista e kontrollit
16. Përfundim

1. Hyrje

Jetojmë në një botë ku pothuajse gjithçka është e lidhur — puna, komunikimi, financa. Kjo lidhshmëri sjell përfitime të mëdha, por edhe rreziqe të reja që të gjithë duhet t'i kuptojmë.

Siguria kibernetike nuk është vetëm detyrë e ekspertëve teknikë. Secili prej nesh, përmes zakoneve tona të përditshme digjitale, kontribuon në sigurinë ose në cenueshmërinë e organizatës. Ky doracak do t'ju japë një kuptim bazë të kërcënimeve dhe zakone praktike për mbrojtje.

Nuk duhet të jeni ekspert teknik për të qenë të sigurt. Duhet vetëm të zhvilloni vetëdije, skepticizëm të shëndetshëm dhe disa zakone të mira. Kjo mjafton për t'i shmangur pjesën më të madhe të kërcënimeve.

Pse është e rëndësishme. Sulmet kibernetike nuk zgjedhin — mund ta godasin këdo. Por përdoruesi i informuar dhe i vëmendshëm është cak shumë më i vështirë. Njohuria është mbrojtja juaj më e mirë.

2. Çfarë është siguria kibernetike

Siguria kibernetike është praktika e mbrojtjes së sistemeve, rrjeteve, pajisjeve dhe të dhënave nga sulmet digjitale. Qëllimi është të sigurohet konfidencialiteti, integriteti dhe disponueshmëria e informacioneve.

2.1 Pse është e rëndësishme për të gjithë

- I mbron të dhënat tuaja personale dhe të punës;
- Parandalon humbjet financiare dhe vjedhjen e identitetit;
- Siguron punë të pandërprerë të organizatës;
- E mbron infrastrukturën kritike nga e cila varet shoqëria.

2.2 Faktori njerëzor

Pjesa e madhe e sulmeve të suksesshme e shfrytëzojnë natyrën njerëzore — kureshtjen, besimin, frikën, dëshirën për të ndihmuar. Teknologjia mund të mbrojë shumë, por vendimi përfundimtar shpesh është i juaji.

Fakt. Pjesa më e madhe e incidenteve të sigurisë përfshijnë gabim njerëzor. Pikërisht për këtë, vetëdija dhe vëmendja juaj janë kyçe.

3. Peizazhi i kërcënimeve moderne

Kërcënimet janë të ndryshme dhe evoluojnë vazhdimisht. Ja më të shpeshtat:

Kërcënimi	Përshkrimi
Softuer keqdashës	Viruse, krimba, trojanë që dëmtojnë sistemet
Ransomware	I kyç të dhënat dhe kërkon shpërblim
Phishing	Mashtrim përmes mesazheve të rreme
Inxhinieria sociale	Manipulim i njerëzve për zbulim informacionesh
Vjedhja e identitetit	Keqpërdorim i të dhënave personale
Sulmet ndaj fjalëkalimeve	Përpjekje për hamendësim ose vjedhje të fjalëkalimeve

4. Softueri keqdashës

Softueri keqdashës (malware) është çdo program i krijuar për të dëmtuar, për të vjedhur të dhëna ose për qasje të paautorizuar në një sistem.

4.1 Llojet

Lloji	Sjellja
Virusi	Ngjitet në skedarë dhe përhapet
Krimbi	Përhapet vetë nëpër rrjete
Trojani	Maskohet si program legjitim
Softueri spiun	Mbledh fshehurazi informacione
Softueri reklamues	Shfaq reklama të padëshiruara

4.2 Si përhapet

- ✓ Bashkëngjitje të infektuara në email
- ✓ Linqe dhe ueb-faqe keqdashëse
- ✓ Pajisje USB të infektuara
- ✓ Softuer pirat ose i pamiratur
- ✓ Sisteme të papërditësuara me dobësi sigurie

4.3 Mbrojtja

- ✓ Mbani antivirus aktiv dhe të përditësuar
- ✓ Përditësoni rregullisht sistemin operativ
- ✓ Mos instaloni softuer të pamiratur
- ✓ Kini kujdes me bashkëngjitjet dhe linqet
- ✓ Mos lidhni pajisje USB të panjohura

5. Ransomware — kyçja e të dhënave për shpërblim

Ransomware është lloj veçanërisht i rrezikshëm i softuerit keqdashës që i enkripton të dhënat tuaja dhe kërkon shpërblim për t'i zhblokuar. Mund ta paralizojë tërë punën.

5.1 Si funksionon

Pas infektimit, ransomware i kyç skedarët dhe shfaq një mesazh me kërkesë për pagesë, më së shpeshti në kriptovalutë, në këmbim të çelësit për zhblokim.

E rëndësishme. Pagesa e shpërblimit nuk garanton kthimin e të dhënave dhe e nxit krimin. Mbrojtja më e mirë është parandalimi dhe kopjet e rregullta rezervë.

5.2 Mbrojtja

- ✓ Bëni kopje të rregullta rezervë të të dhënave të rëndësishme
- ✓ Mos hapni bashkëngjitje ose linqe të dyshimta
- ✓ Mbajini sistemet të përditësuara
- ✓ Raportoni menjëherë nëse vëreni enkriptim të pazakontë të skedarëve

6. Inxhinieria sociale

Inxhinieria sociale është manipulimi i njerëzve që të zbulojnë informacione konfidenciale ose të ndërmarrin veprime që e rrezikojnë sigurinë. Në vend që ta sulmojnë teknologjinë, sulmuesit e sulmojnë natyrën njerëzore.

6.1 Teknikat e shpeshta

Teknika	Përshkrimi
Paraqitja e rreme	Shtirja si person ose institucion i besueshëm
Urgjenca	Krijimi i presionit për reagim të shpejtë, të pamenduar
Autoriteti	Paraqitja si epror ose autoritet
Ndihma	Shfrytëzimi i dëshirës për të ndihmuar
Kureshtja	Karrema që e nxisin kureshtjen

Mbrojtja. Skepticizmi i shëndetshëm është kyç. Nëse diçka duket urgjente, e pazakontë ose tepër e mirë për të qenë e vërtetë — ndaluni dhe verifikoni përmes një kanali të pavarur.

7. Siguria e fjalëkalimeve dhe e llogarive

Fjalëkalimet janë çelësat e jetës suaj digjitale. Mbrojtja e tyre është themeli i sigurisë kibernetike.

- ✓ Përdorni fjalëkalime të gjata (së paku 12 karaktere)

- ✓ Kombinoni shkronja, numra dhe simbole
- ✓ Fjalëkalim unik për çdo llogari
- ✓ Përdorni menaxher fjalëkalimesh
- ✓ Aktivizoni autentifikimin me dy faktorë kudo që është i disponueshëm
- ✓ Kurrë mos ndani fjalëkalime

Këshillë. Autentifikimi me dy faktorë është një nga mbrojtjet më efikase. Edhe nëse fjalëkalimi komprometohet, faktori i dytë e parandalon kyçjen e paautorizuar.

8. Shfletim i sigurt në internet

- ✓ Kontrolloni a fillon adresa me "https" për faqet e ndjeshme
- ✓ Kini kujdes me ueb-faqet e dyshimta ose të panjohura
- ✓ Mos shkarkoni skedarë nga burime të pabesueshme
- ✓ Kini kujdes me reklamat e rreme dhe dritaret pop-up
- ✓ Mbajeni shfletuesin të përditësuar

9. Pajisjet mobile dhe siguria

Telefonat e mençur dhe tabletët përmbajnë shumë informacione të ndjeshme dhe janë cak i shpeshtë.

- ✓ Kyçeni pajisjen me PIN, fjalëkalim ose biometri
- ✓ Instaloni aplikacione vetëm nga dyqanet zyrtare
- ✓ Kini kujdes ndaj lejeve që i kërkojnë aplikacionet
- ✓ Mbajeni sistemin operativ të përditësuar
- ✓ Mos e lini pajisjen pa mbikëqyrje
- ✓ Mundësoni fshirjen në distancë në rast humbjeje

10. Siguria në rrjetet publike

Wi-Fi publik (kafene, aeroporte, hotele) është i përshtatshëm, por sjell rreziqe. Sulmuesit mund ta përgjojnë trafikun në rrjetet e pambrojtura.

- ✓ Përdorni VPN në rrjetet publike
- ✓ Shmangni transaksionet e ndjeshme në Wi-Fi publik
- ✓ Çaktivizoni lidhjen automatike me rrjetet e hapura
- ✓ Kontrolloni emrin e rrjetit — sulmuesit krijojnë të rreme

Rregull. Mos u qasni në sisteme të ndjeshme dhe mos vendosni fjalëkalime përmes Wi-Fi-t publik pa VPN. Gjithmonë përdorni VPN për lidhje të sigurt.

11. Mbrojtja e privatësisë

- ✓ Kini kujdes çfarë ndani në rrjetet sociale
- ✓ Shqyrtojini cilësimet e privatësisë
- ✓ Mos publikoni informacione të ndjeshme personale ose të punës
- ✓ Kini kujdes — informacionet që i publikoni mund të përdoren kundër jush

12. Kopjet rezervë dhe rikuperimi

Kopjet rezervë janë rrjeta juaj e sigurisë. Nëse të dhënat humben për shkak të një sulmi, defekti ose gabimi, kopja mundëson rikthimin.

- ✓ Bëni kopje të rregullta rezervë të të dhënave të rëndësishme
- ✓ Ruajini kopjet në vend të sigurt, të ndarë
- ✓ Kontrolloni që kopjet funksionojnë
- ✓ Ndiqni rekomandimin e Sektorit të TI-së për mënyrën e arkivimit

13. Skenarë praktikë

Skenari 1: Thirrje urgjente për "mbështetje teknike"

Ju thërret dikush që pretendon se është nga mbështetja teknike dhe se kompjuteri juaj është i infektuar. Kërkon të instaloni një program për qasje në distancë që ta "rregullojë".

Reagimi i drejtë: Nuk instaloni asgjë dhe nuk jepni qasje. Mbështetja legjitime nuk ju thërret papritur në këtë mënyrë. E ndërprisni dhe raportoni te Sektori i vërtetë i TI-së.

Skenari 2: Dhuratë falas

Merrni njoftim se keni fituar një shpërblim dhe duhet të vendosni të dhëna personale për ta marrë.

Reagimi i drejtë: E injoroni. Nëse diçka është tepër e mirë për të qenë e vërtetë, ka shumë të ngjarë të jetë mashtrim. Nuk vendosni asnjë të dhënë.

Skenari 3: Aplikacion i dyshimtë

Gjeni një aplikacion që premtan funksion të dobishëm, por kërkon qasje në kontakte, mesazhe dhe lokacion edhe pse kjo nuk nevojitet për qëllimin e tij.

Reagimi i drejtë: Nuk e instaloni. Lejet e tepërta janë shenjë e një aplikacioni të dyshimtë. Instaloni vetëm nga burime zyrtare.

14. Pyetjet më të shpeshta

A më mbron plotësisht antivirusi?

Jo. Antivirusi është shtresë e rëndësishme, por jo e mjaftueshme vetë. Vëmendja juaj, sistemet e përditësuara dhe zakonet e mira janë po aq të rëndësishme.

Çfarë është më e rëndësishme për sigurinë kibernetike?

Vetëdija. Shumica e sulmeve e kërkojnë pjesëmarrjen tuaj (klik, vendosje të dhënash). Përdoruesi i vëmendshëm e shmang pjesën më të madhe të kërcënimeve.

Sa shpesh duhet ta ndryshoj fjalëkalimin?

Kur ka dyshim për komprometim, dhe për llogaritë kritike periodikisht. Më e rëndësishme se ndryshimi i shpeshtë është që fjalëkalimi të jetë i fortë, unik dhe i mbrojtur me 2FA.

A është e sigurt të përdor kompjuterë publikë?

Me kujdes të madh. Mos vendosni fjalëkalime për llogari të ndjeshme, gjithmonë çkyçuni dhe mos lini të dhëna personale. Sipas mundësisë, shmangini për punë të rëndësishme.

Po nëse mendoj se jam i infektuar?

Ndërpriteni lidhjen me internetin, mos vendosni fjalëkalime dhe raportoni menjëherë te Sektori i TI-së. Reagimi i shpejtë e kufizon dëmin.

15. Fjalorthi dhe lista e kontrollit

Termi	Kuptimi
Malware	Softuer keqdashës — term i përgjithshëm për programet e dëmshme
Ransomware	Softuer që i kyç të dhënat dhe kërkon shpërblim
Trojani	Program keqdashës i maskuar si legjitim
Inxhinieria sociale	Manipulim i njerëzve për zbulim informacionesh
VPN	Rrjet privat virtual për lidhje të sigurt
Autentifikimi me dy faktorë	Shtresë e dytë mbrojtjeje gjatë kyçjes
Kopja rezervë	Kopje e të dhënave për rikthim në rast humbjeje

Higjiena bazë kibernetike

- ✓ Fjalëkalime të forta dhe unike + 2FA
- ✓ Sisteme dhe antivirus të përditësuar
- ✓ Kujdes me email, linqe dhe bashkëngjitje
- ✓ VPN në rrjetet publike

- ✓ Kopje të rregullta rezervë
- ✓ Raportim i çdo dyshimi

Siguria kibernetike edhe jashtë punës

Zakonet e mira për siguri kibernetike nuk mbarojnë kur e lëshoni vendin e punës. Mbrojtja e jetës suaj digjitale në shtëpi është po aq e rëndësishme — dhe shpesh të njëjtat parime ju mbrojnë edhe në punë edhe privatisht.

Rrjeti shtëpiak

- ✓ Ndryshojeni fjalëkalimin standard të ruterit shtëpiak
- ✓ Përdorni fjalëkalim të fortë për Wi-Fi-n shtëpiak
- ✓ Përditësojeni ruterin kur ka përditësime të disponueshme
- ✓ Ndani rrjet të veçantë për mysafirë

Mbrojtja e familjes

- ✓ Bisedoni me familjen për rreziqet kibernetike
- ✓ Ndihmojuni t'i njohin mashtrimet
- ✓ Kini kujdes për sigurinë e fëmijëve në internet
- ✓ Mbajini pajisjet shtëpiake të përditësuara dhe të mbrojtura

Kulturë e përbashkët. Siguria kibernetike është mënyrë e të menduarit, jo grup rregullash vetëm për punën. Kur bëhet zakon në çdo aspekt të jetës, ju dhe të afërmit tuaj jeni shumë më të sigurt.

Mësim i vazhdueshëm

Teknologjia dhe kërcënimet ndryshojnë vazhdimisht. Qëndroni të informuar, ndiqni rekomandimet dhe mos hezitoni të pyesni kur jeni në dilemë. Mësimi për sigurinë kibernetike është udhëtim që zgjat tërë jetën.

16. Përfundim

Siguria kibernetike është proces i vazhdueshëm, jo aktivitet i njëhershëm. Kërcënimet do të ndryshojnë, por parimet themelore mbeten: jini të kujdesshëm, skeptikë ndaj të papriturës dhe mbani zakone të mira digjitale.

Mesazhi kyç. Ju jeni linja më e rëndësishme e mbrojtjes. Çdo vendim i informuar që e merrni e rrit sigurinë tuaj dhe të tërë organizatës.

MEPSO SHA Shkup — Operatori i sistemit të transmetimit të energjisë elektrike të Maqedonisë së Veriut
Dokument nr. MEPSO-PRI-SAJ-003 · Klasifikimi: Përdorim i brendshëm
Ky doracak është pronë e MEPSO SHA dhe është i dedikuar për trajnim dhe përdorim të brendshëm.