UK International Development
Partnership | Progress | Prosperity

Media Diversity Institute

All Rights Foundation

CyberHUB

ՍԹԱՓ | Ստանդարտ. Թվային Անվտանգության Փաթեթ

Թվային անվտանգության քաղաքականությունների ստանդարտներ հասարակական կազմակերպությունների համար

Երևան, 2025

@mdiarmenia
@cyberhubam
@allrights

ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆՆԵՐԻ ՍՏԱՆԴԱՐՏ

ՍԹԱՓ | Ստանդարտ. Թվային Անվտանգության Փաթեթ

Կիբեռանվտանգության ստանդարտ հասարակական կազմակերպությունների համար

Այս փաստաթուղթը մշակվել է «Թվային անվտանգության ազգային ստանդարտներ ՔՀԿ-ների համար» ծրագրի շրջանակում, որը ֆինանսավորվում է Միացյալ Թագավորության միջազգային զարգացման աջակցության շրջանակում՝ ՄԹ կառավարության կողմից:

Ծրագիրն իրականացվում է Բազմակողմանի տեղեկատվության ինստիտուտի, CyberHUB նախաձեռնության և Բոլորը հանուն հավասար իրավունքների հիմնադրամի կողմից:

www.mdi.am
www.cyberhub.am
www.allrights.am

Երևան, 2025

Ներածություն

Կիբեռանվտանգության այս քաղաքականությունը սահմանում է գործողությունների ուղեցույց, որը պաշտպանում է կազմակերպության տվյալները, ցանցը և տեղեկատվական համակարգերը կիբեռսպառնալիքներից: Այն մշակված է **մատչելի կիրառելիության** սկզբունքով, որի օգտագործման պայմաններից է դրա **պարբերական թարմացումը**:

- **Թարմացման պարբերականություն.** այս քաղաքականությունը վերանայվում է **ամեն տարի** կամ **հիմնական վարչական-ադմինիստրատիվ փոփոխությունների ժամանակ** (օրինակ՝ գրասենյակի վայրի փոփոխություն, մեծ քանակի նոր աշխատակիցների ներգրավում և այլն):
- **Կիրառելիություն**. քաղաքականությունը կիրառվում է բոլոր աշխատակիցների, կամավորների, պայմանագրային իրավահարաբերության մեջ գտնվող ցանկացած անձանց և խորհրդատուների համար, որոնք ունեն մուտք դեպի կազմակերպության համակարգեր և տվյալներ:

---

1. Անվտանգ կարգավորումներ

Նպատակ
Նպաստել համակարգերի և սարքերի անվտանգ կարգավորմանը՝ բացառելով ավելորդ և չհավաստագրված ծրագրերի և ծառայությունների կիրառումը, որոնք կարող են հանդիսանալ խոցելիություններ հնարավոր հարձակումների համար:

Քաղաքականություն

- **Համակարգի կարգավորում**. ռիսկերը նվազեցնելու համար անհրաժեշտ է **անջատել կամ հեռացնել ավելորդ և չհավաստագրված ծրագրեր ծրագրերը**, ծառայությունները և օգտագործողների հաշիվները:

- **Ավտոմատ գործարկման անջատում**. փակել «auto-run» կամ «auto-play» ֆունկցիաները համակարգիչներում՝ ֆայլերի ինքնաբերաբար գործարկումը կանխելու համար:

- **Մուտքի/հասանելիությունների վերահսկում**. ապահովել յուրաքանչյուր աշխատակցի նվազագույն անհրաժեշտ արտոնությունները, որոնք պետք են լիազորությունների կատարման համար:

Ինչպե՞ս կիրառել (How-To)

1. Հետազոտեք համակարգչի, հեռախոսի ծրագրերի և հավելվածների ցանկը, հեռացրեք այն ծրագրերը, որոնք ձեզ պետք չեն:
2. Windows համակարգերում կարող եք «Turn Windows Features on or off» բաժնում անջատել ավելորդ ֆունկցիոնալները: Linux-ում՝ օգտագործեք «systemctl disable service_name» կամ «package manager»-ները:[1]
3. Պարբերաբար, օրինակ, ամսական մեկ անգամ ստուգեք և/կամ վերանայեք բոլոր աշխատակիցների հաշիվները և դրանց համապատասխանությունը իրենց տրված

լիազորություններին: Հեռացրեք կամ չեղարկեք նախկին աշխատակիցներին պատկանող արտոնությունները/հաշիվները:

Գործնական օրինակներ

- **Ubuntu/Linux**. ենթադրենք ունեք MySQL, բայց իրականում տվյալների բազա չեք օգտագործում. կարելի է ծառայության (service) ավտոմատ գործարկումն անջատել «stop/disable» հրամանով:
- **Windows**.[2] եթե ձայնասկավառակ (CD/DVD) չեք օգտագործում, ապա անջատեք Auto-play-ը, որպեսզի արտաքին կրիչի մեջ վիրուսային ֆայլերը ինքնաբերաբար չաշխատեն:

Լրացուցիչ ռեսուրսներ

- Անվճար կամ զեղչված արժեքով ծրագրային ապահովումներ հասարակական կազմակերպությունների համար - TechSoup
- Անվճար և բաց կոդով օպերացիոն համակարգեր - Ubuntu կամ Linux Mint

---

2. Անվտանգության թարմացումների կառավարում

Նպատակ

Նպաստել թարմացումների կառավարմանը և իրականացմանը՝ գոյություն ունեցող և նորաստեղծ ռիսկերը մեղմացնելու կամ չեզոքացնելու համար:

Քաղաքականություն

- **Ավտոմատ թարմացումներ**. բոլոր օպերացիոն համակարգերում, հավելվածներում և ծրագրային ապահովումներում անհրաժեշտ է ակտիվացնել ավտոմատ թարմացումները:

- **Թարմացումների ժամանակացույց**. **կրիտիկական** կամ **բարձր ռիսկային** թարմացումները անհրաժեշտ է իրականացնել **14 օրվա ընթացքում**:

- **Ինքնուրույն (manually) թարմացումներ**. այն համակարգերի համար, որտեղ ավտոմատ թարմացումը հնարավոր չէ, անհրաժեշտ է պարբերաբար ստուգել (օր.՝ ամեն շաբաթ) և ինքնուրույն իրականացնել դրանք:

- **Վերահսկում**. պարբերաբար պետք է ստուգել (օրինակ՝ ամսական), արդյոք թարմացումները **ակտիվ են**: Պետք է կանխել այն դեպքերը, երբ աշխատակիցներն անջատում են թարմացումները սարքավորման հիշողության/տեղի պակասի կամ այլ պատճառով:

Ինչպե՞ս կիրառել (How-To)

1. Windows-ում բացեք «Settings» → «Update & Security» և համոզվեք, որ «Updates»-ը ակտիվ է:
2. macOS-ում անցեք «System Preferences» → «Software Update»:

3. Linux-ում, կախված բաշխումից (Ubuntu/Debian/Red Hat), օգտագործեք «apt-get update», «apt-get upgrade» կամ համապատասխան «package manager»:
4. Հեռախոսների վրա (Android/iOS) միացրեք ավտոմատ թարմացումը «Settings» բաժնից:

Գործնական օրինակ

- Եթե ձեր կազմակերպությունը դեռ օգտագործում է Windows 7, ապա անհրաժեշտ է անցնել Windows 10/11 կամ Linux, քանի որ Windows 7-ում անվտանգության նոր թարմացումներ չեն իրականացվում:

Լրացուցիչ ռեսուրսներ

- Ավտոմատ թարմացումներ իրականացնելու գործիքներ Windows-ի համար - Secunia PSI կամ Patch My PC

---

3. Պաշտպանություն վնասակար ծրագրերից (Malware)

Նպատակ
Նպաստել սարքավորումների անվտանգությանը վիրուսներից, լրտեսող ծրագրերից, կոդավորող (ransomware) ծրագրերից և այլ վնասակար ծրագրերից:

Քաղաքականություն

- **Հակավիրուսային (Anti-Malware) ծրագիր**. տեղադրել վստահելի հակավիրուսային ծրագիր (օրինակ՝ Windows Defender, Avast, Bitdefender և ClamAV՝ Linux-ի համար):

- **Պարբերական թարմացումներ**. պետք է համոզվել, որ հակավիրուսային տվյալների շտեմարանները թարմացված են:

- **Պլանավորված սկանավորում**. առնվազն շաբաթական մեկ անգամ անհրաժեշտ է իրականացնել համակարգի լրիվ (full) սկանավորում:

- **Սպիտակ ցանկ (Whitelisting)**. հնարավորության դեպքում թույլատրել միայն հաստատված ծրագրերի գործարկումը:

- **Օգտագործել օպերացիոն համակարգի հակավիրուսային համակարգերը.** եթե չկան համապատասխան ռեսուրսներ հակավիրուսային ծրագրերի տեղադրման համար, ապա անհրաժեշտ է հետևել, որպեսզի Windows, MacOS համակարգերում ներդրված անվտանգային համակարգերը միշտ ակտիվացված և թարմացված լինեն: Դրանք նույնպես արդյունավետ են բազային անվտանգությունն ապահովելու համար:

- **Օգտատերերի վերապատրաստում**. պետք է կազմակերպել ուսուցումներ, որպեսզի աշխատակիցները ճանաչեն ֆիշինգային (phishing) նամակները և բացառեն չարամիտ ֆայլերի ներբեռնումը: Պետք է ստեղծել համակարգ, որի միջոցով աշխատակիցները կկարողանան հաղորդել ղեկավարությանը՝

նմանօրինակ վնասակար նամակներ հայտնաբերելիս։

Ինչպե՞ս կիրառել (How-To)

1. Ընտրեք և տեղադրեք վստահելի հակավիրուսային ծրագրեր կամ ակտիվացրեք օպերացիոն համակարգերի ներդրվածները։
2. Շաբաթական կտրվածքով կարգավորեք պլանավորված (scheduled) ստուգումները։
3. Կասկածելի նամակներ ստանալիս մի բացեք կցված ֆայլերը և հղումները մինչև չհամոզվեք դրանց անվտանգության հարցում։

Գործնական օրինակ

- Եթե աշխատելիս օգտագործում եք հանրային Wi-Fi, ապա օգտագործեք VPN, որպեսզի չարամիտ ծրագրերը կամ այլ օգտատերերը չկարողանան հեշտությամբ հասանելիություն ունենալ ձեր տվյալներին։

Լրացուցիչ ռեսուրսներ

- Անվճար բաց կոդով հակավիրուս Linux/Mac/Windows-ի համար - ClamAV
- Չարամիտ ծրագրեր հայտնաբերելու գործիք, որը պահանջում է խորացված գիտելիքներ կիրառման համար - Malwarebytes

---

4. Օգտատերերի մուտքի վերահսկում

Նպատակ

Նպաստել աշխատակիցների պարտականություններին համապատասխան մուտքի իրավունքին՝ անհարկի հասանելիությունները կանխելու նպատակով։

Քաղաքականություն

- **Նվազագույն արտոնություն**. յուրաքանչյուր օգտատեր պետք է ստանա մուտքի և գործողությունների այն նվազագույն իրավունքները և լիազորությունները, որոնք անհրաժեշտ են իր աշխատանքի համար։

- **Անհատական հաշիվներ**. չի կարելի օգտագործել ընդհանուր (shared) հաշիվներ։ Յուրաքանչյուր աշխատակից պետք է ունենա իր **յուրահատուկ/առանձին** անուն-գաղտնաբառը։

- **Մուտքի վերահսկման վերանայում**. 3-6 ամիսը մեկ անգամ պետք է ստուգել՝ արդյոք օգտատերերի դերերն ու թույլտվությունները համապատասխանում են նրանց իրական աշխատանքին։

- **Բազմափուլային վավերացում (MFA)**. անհրաժեշտ է ակտիվացնել MFA-ը բոլոր այն հաշիվների համար, որոնք մշակման կամ հասանելիության բարձր մակարդակ ունեն, այդ թվում նաև աշխատակիցների անձնական էլ. փոստերը, սոցիալական ցանցերի և մեսենջերների հաշիվները, որոնք օգտագործվում են աշխատանքային հաղորդակցության համար։

- **Մուտքի չեղարկում**. հեռացող աշխատակիցների բոլոր հաշիվները և մուտքերը դեպի ընդհանուր կիրառվող հաշիվներ (օրինակ՝ կազմակերպության Facebook-ում էջի կառավարման տարբերակները) պետք է անմիջապես փակել։

Ինչպե՞ս կիրառել (How-To)

1. Ստեղծեք օգտատիրոջ անուն-գաղտնաբառ յուրաքանչյուր նոր աշխատակցի համար։ Մի օգտագործեք ընդհանուր «Admin» կամ «User» հաշիվներ։
2. Պարբերաբար (օրինակ՝ եռամսյակը մեկ) ստուգեք, թե ինչ օգտատերեր կան համակարգում։ Հեռացրեք նրանց, որոնք այլևս չեն աշխատում։
3. MFA-ի դեպքում (օրինակ՝ Google Authenticator, Microsoft Authenticator, կամ անվտանգության բանալի / security key) խուսափեք SMS-based տարբերակից, եթե հասանելի են ավելի անվտանգ եղանակներ։

Գործնական օրինակ

- Եթե ձեր կազմակերպությունն ունի համակարգեր, որոնք ղեկավարվում են անհատ օգտատերերի կողմից (սոցցանցեր, CRM, տվյալների շտեմարաններ և այլն), ապա համոզվեք, որ կառավարող բոլոր օգտատերերը հանդիսանում են տվյալ պահին գործող աշխատակիցներ։ Նաև համոզվեք, որ այնտեղ գրանցումների համար աշխատակիցների կողմից չեն օգտագործվում անձնական չպաշտպանված էլեկտրոնային փոստի հասցեներ։

Լրացուցիչ ռեսուրսներ

- MFA-ի համար նախատեսված հավելվածներ - Authy, Google Authenticator, Microsoft Authenticator

---

5. Գաղտնաբառերի և վավերացման ստանդարտներ

Նպատակ
Նպաստել ուժեղ գաղտնաբառերի և վավերացման միջոցառումների կիրառմանը՝ հաշիվները չարտոնված մուտքերից պաշտպանելու համար։

Քաղաքականություն

- **Գաղտնաբառերի պահանջներ**. պետք է մշակել 12+ նիշից բաղկացած, պարզ հաջորդականություններից զերծ (օր.՝ 12345, password) գաղտնաբառեր։ Գաղտնաբառերը ստեղծելիս չի կարելի օգտագործել կռահելի բաղադրիչներ (օրինակ՝ սեփական, երեխաների կամ ընտանիքի այլ անդամների անունները, ծննդյան տարեթվերը, հեռապոսահամարները)։ Յուրաքանչյուր հաշվի համար պարտադիր է կիրառել **տարբերվող** գաղտնաբառեր։

- **Գաղտնաբառերի կառավարում**. անհրաժեշտ է հորդորել օգտատերերին օգտագործել գաղտնաբառերի կառավարիչ (password manager), որպեսզի խուսափեն

«մեկ գաղտնաբառ ամեն տեղ» մոտեցումից: Պարբերաբար պետք է համոզվել, որ գաղտնաբառերի կառավարիչն օգտագործվում է բոլոր աշխատակիցների կողմից:

- **Բազմափուլային վավերացում (MFA)**. բոլոր հիմնական հաշիվներում (գերադասելի է բոլոր հաշիվների վրա) ակտիվացնել 2FA (երկփուլ) կամ MFA (բազմափուլ) վավերացում:

- **Գաղտնաբառի փոփոխում**. Յուրաքանչյուր տարի անհրաժեշտ է թարմացնել գաղտնաբառերը, ավելի հաճախ՝ կասկածների դեպքում: Չի խրախուսվում առավել հաճախ և պարտադրված փոխել գաղտնաբառերը, օրինակ, ամեն ամիս, քանի որ դա բերում է աշխատակիցների կողմից թույլ գաղտնաբառերի կիրառման:

Ինչպե՞ս կիրառել (How-To)

1. Ընտրեք ձեզ համար ցանկալի և կիրառելի Password Manager (օրինակ՝ KeePass, Bitwarden, ProtonPass կամ այլ) և աշխատակիցներին տրամադրեք հակիրճ ուղեցույց դրանց կիրառման վերաբերյալ:

Գործնական օրինակ

- Եթե աշխատակիցը նույն գաղտնաբառն է օգտագործում իր անձնական Gmail-ի և ներքին/աշխատանքային համակարգերի համար, ապա որևէ ֆիշինգային հարձակում ուղղված իր Gmail-ին, կարող է վնասել նաև ձեր կազմակերպությանը:

Լրացուցիչ ռեսուրսներ

- Բաց կողով և անվճար տարբերակ ունեցող գաղտնաբառերի կառավարիչ - Bitwarden
- Օֆլայն գաղտնաբառերի կառավարիչ Windows/Linux/Mac օպերացիոն համակարգերով աշխատող համակարգիչների համար - KeePass

---

6. Ադմինիստրատիվ հաշիվներ (Administrative Accounts)

Նպատակ

Նպաստել վերահսկողության խստացմանն այն հաշիվների նկատմամբ, որոնք տրամադրում են լայն (admin-level) իրավունքներ:

Քաղաքականություն

- **Առանձին հաշիվներ ադմինիստրատորների համար**. ադմինիստրատորները պետք է ունենան առանձին «admin» և «user» հաշիվներ:

- **Արտոնությունների սահմանափակում**. միայն ադմին մակարդակի (admin-level) գործողությունների կարիք ունեցող աշխատակիցները պետք է ունենան համապատասխան հասանելիություն և լիազորությունների շրջանակ: Ադմինիստրատորի և աշխատակիցների կողմից իրականացվող գործողությունները պետք է գրանցվեն և ժամանակ առ ժամանակ ստուգվեն: Բոլոր մնացած օգտատերերը, որոնք ունեն որոշակի սահմանափակումներ, պետք է

օգտվեն «user» հաշիվներից:

- **Պարբերական վերահսկում**. երեք ամիսը մեկ պետք է ստուգել, թե ով ունի «admin-level»: Եթե ադմինիստրատորի (համապատասխան աշխատակցի) գործառույթները փոխվել են, ապա պետք է ազատել «admin-level»-ից:

- **Մուտքի չեղարկում**. երբ աշխատակիցը հեռանում է, նրա «admin-level» արտոնությունները պետք է անմիջապես չեղարկվեն:

Ինչպե՞ս կիրառել (How-To)

1. Ստեղծեք յուրաքանչյուրի համար երկու հաշիվ (user_lilit և admin_lilit), և ամենօրյա աշխատանքում մի կիրառեք «admin_lilit» հաշիվը:
2. Պահեք «audit logs»-ը (Windows Event Viewer, Linux syslog), որպեսզի հնարավորություն ունենաք հետագայում տեսնել, թե ով ինչ փոփոխություններ է կատարել համակարգում:

Գործնական օրինակ

- Պայմանական, եթե ձեր կազմակերպությունում կա 5 աշխատակից, կարևոր է, որ ոչ բոլորը լինեն «admin», ինչը խիստ ռիսկային է: Ավելի ապահով է, երբ միայն 1-2 հոգի ունի «admin-level», իսկ մյուսները գործեն սովորական՝ «user» իրավունքներով:

Լրացուցիչ ռեսուրսներ

- **NIST Special Publication 800-53.** ադմինիստրատիվ հաշիվների անվտանգության կառավարման և վերահսկման (access control) լավագույն փորձառություններ - Security and Privacy Controls for Information Systems and Organizations

- **CIS Controls (Center for Internet Security).** ադմինիստրատիվ հաշիվների կառավարումն ապահովող քայլեր և լավագույն փորձ (Role-based access, MFA, audit logs և այլն) - Implementation Guide for Administrative Access and Account Management

- **Microsoft Docs – Local Administrator Accounts.** Windows միջավայրում լոկալ ադմինիստրատորների հաշիվների անվտանգ համակարգում, ներառյալ Group Policy-ների և LAPS-ի (Local Administrator Password Solution) կարգավորումներ - Կարդալ առցանց[3]

- **Linux Sysadmin – Privileged Access Management.** սահմանափակ «root» մուտք «Ubuntu», «Debian», «CentOS» օպերացիոն համակարգերում, «sudo»-ի և «audit log»-ի ճիշտ կառավարում, և միայն անհրաժեշտ անձանց լիազորում sudo արտոնություններ: Եզրակացությունները կիրառելի են նաև այլ Linux-ի բաշխումների համար - Arch Linux Wiki on sudo

7. Միջադեպերի արձագանքման պլան

Նպատակ
Նպաստել կիբեռմիջադեպերի հետևանքների/վնասի նվազեցմանը՝ գործողությունների հստակ պլանի միջոցով:

Քաղաքականություն

- **Արձագանքման պլան**. կազմակերպությունը պետք է ունենա գրավոր պլան, որտեղ նշված է, թե միջադեպերի դեպքում աշխատակիցները առաջնահերթ ում հետ պետք է կապ հաստատեն, ինչ քայլեր պետք է կատարել հարձակումը զսպելու, տվյալները և/կամ հասանելիությունը վերականգնելու համար:

- **Արձագանքման թիմ**. անհրաժեշտ է նշանակել կոնկրետ պատասխանատուների և իրականացնել դերաբաշխում (օրինակ՝ SS պատասխանատու, Հաղորդակցության պատասխանատու, Իրավական հարցերով պատասխանատու և այլն): Փոքր կազմակերպություններում մեկ աշխատակիցը կարող է ունենալ մի քանի դեր:

- **Վերապատրաստումներ**. տարեկան 1-2 անգամ անհրաժեշտ է կատարել վարժանքներ և սիմուլյացիաներ՝ ինչպես կվարվեին աշխատակիցները ֆիշինգի, ransomware հարձակման կամ այլ դեպքերում:

- **Միջադեպերի փաստաթղթավորում**. պետք է ապահովել, որ յուրաքանչյուր միջադեպ գրանցվի, վերլուծվի և պահպանվի հետագա փորձի զարգացման համար (քաղված դասեր):

Ինչպե՞ս կիրառել (How-To)

1. Ստեղծեք սեղմ/արագ արձագանքող և պարզ հաղորդակցության սխեմա. օրինակ, եթե կա միջադեպ, ապա առաջին հերթին զանգահարեք SS պատասխանատուին, հետո ղեկավարին և կապվեք հասարակական կազմակերպություններին թվային պաշտպանություն տրամադրող տեղական կամ միջազգային կազմակերպությունների հետ:
2. Մշակեք հետ-միջադեպային փաստաթուղթ (Post-incident Analysis), որում կնշեք, թե ինչ ապացույցներ են հայտնաբերվել, ինչպես է լուծվել խնդիրը, ինչպես է հնարավոր բարելավել հետագա անվտանգությունը և բացառել կամ նվազեցնել նմանօրինակ կիբեռմիջադեպերը:

Գործնական օրինակ

- Ransomware [4] հարձակման դեպքում նախ անջատեք վարակված համակարգիչը ներքին ցանցից և ինտերնետից, որպեսզի այն չտարածվի, և անմիջապես կապվեք թվային անվտանգության մասնագետների հետ:

Լրացուցիչ ռեսուրսներ

- Հայաստանում գործող քաղաքացիական հասարակության և մեդիա կազմակերպություններին թվային աջակցություն և խորհրդատվություն

տրամադրող թիմ - CyberHUB
- Թվային աջակցության միջազգային ծառայություն - AccessNow Help

---

8. Կրթություն և իրազեկում

Նպատակ
Նպաստել աշխատակիցների իրազեկվածությանն ու շարունակական կրթությանը՝ կազմակերպության ընդհանուր անվտանգությունը բարձրացնելու և սխալների հավանականությունը նվազեցնելու նպատակով:

Քաղաքականություն

- **Շարունակական կրթություն**. տարեկան կտրվածքով կազմակերպել կիբեռանվտանգության պարտադիր ուսուցում բոլորի համար:

- **Թիրախային կրթություն**. այն աշխատակիցները, որոնք աշխատում են առավել ռիսկային կամ զգայուն տվյալների հետ, պետք է ստանան ավելի խորացված գիտելիք:

- **Պարբերական հիշեցումներ**. 1-3 ամիսը մեկ (ըստ կազմակերպության կարիքների) պետք է ուղարկել էլեկտրոնային նամակ-հուշումներ կամ իրականացնել փոքր հանդիպումներ, որտեղ անհրաժեշտ է քննարկել նոր ռիսկերն ու դրանց կանխարգելման եղանակները:

- **Ֆիշինգային սիմուլյացիաներ**. հնարավորության դեպքում պետք է կազմակերպել փոքրիկ «ֆիշինգային հարձակումներ»՝ ուղարկելով փորձնական phishing email՝ տեսնելու համար, թե աշխատակիցներից որոնք կզտնվեն աչալուրջ և որոնք հավելյալ վերապատրաստման կարիք կունենան:

Ինչպե՞ս կիրառել (How-To)

1. Նոր աշխատակիցների համար ներգրավման հատուկ գործընթաց պլանավորեք (**onboarding**), որի ընթացքում կհամոզվեք, որ նա պատրաստ է հիմնական սպառնալիքներին:
2. Մշակեք վերապատրաստման համար կրթական մոդուլներ՝ բազային ուսուցման և միջադեպերի ուսումնասիրման համար:
3. Տարեկան վերապատրաստումից բացի, իրականացրեք փոքր՝ 5-10 րոպեանոց քննարկումներ աշխատանքային ժողովների ընթացքում:

Գործնական օրինակ

- Աշխատակիցների համար ուսուցումը հետաքրքիր դարձնելու նպատակով կարող եք օգտագործել quiz-ի հարթակներ (Kahoot, Quizizz): Սրանք կօգնեն գործընթացը խաղաֆիկացնել և ինտերակտիվ դարձնել:

Լրացուցիչ ռեսուրսներ

- Հոդվածներ և բլոգներ թարմ կիբեռռիսկերի վերաբերյալ - Cyberhub.am
- Անվճար ռեսուրսներ և դասընթացներ թվային անվտանգության վերաբերյալ - Cyber Readiness Institute
- Բաց կոդով գործիքներ ֆիշինգային սիմուլյացիաների համար - Phishing Simulation Tools
- ֆիշինգային նամակների ստեծման ռուսալեզու հարթակ - StopPhish

---

9. Հսկողություն/մշտադիտարկում և աուդիտ (Monitoring and audit)

Նպատակ
Մշտադիտարկման միջոցով նպաստել անսովոր ակտիվության հայտնաբերմանը և աուդիտի միջոցով աջակցել անվտանգության չափանիշների պահպանմանը։

Քաղաքականություն

- **Պարբերական աուդիտ**. առնվազն տարեկան մեկ անգամ պետք է անցկացնել անվտանգության աուդիտ (ներքին կամ արտաքին աուդիտորների ներգրավվմամբ), որտեղ ստուգվում են օգտատերերի իրավունքները, firewall-ի (արգելապատնեշ) կարգավորումները, թարմացումները և այլն։
- **Մուտքի վերահսկում**. երեք ամիսը մեկ պետք է վերանայել, թե ովքեր ունեն մուտքի իրավունքներ կարևոր համակարգեր։
- **Փաստաթղթավորում**. անհրաժեշտ է գրանցել բոլոր արդյունքները, ուղղիչ միջոցառումները և հետագա քայլերը։

Ինչպե՞ս կիրառել (How-To)

1. Կազմեք ստուգաթերթ (checklist), որում կլինեն հիմնական կետերը (թարմացումներ, օգտատերերի իրավունքներ, firewall, հակավիրուս և այլն)։
2. Աուդիտից հետո կազմեք գործողությունների պլան, թե ինչն է պետք շտկել, ինչ ժամկետում և ում կողմից։

Գործնական օրինակ

- Պայմանական, եթե աուդիտի ժամանակ պարզվում է, որ 2 աշխատակից, որոնք 6 ամիս է հեռացել են աշխատանքից, սակայն դեռ ունեն հասանելիություն G-Suite կամ Microsoft 365 համակարգերին, ապա անմիջապես պետք է փակեք այդ հաշիվները։ Եվ ավելի կարևոր է հասկանալ, թե ինչու՞ և ու՞մ պատճառով է ստեղծվել նման իրավիճակ, ինչպե՞ս խուսափել նման դեպքերից հետագայում։

10. Firewall (ֆայերվոլի) և ցանցի անվտանգություն

Նպատակ
Նպաստել կազմակերպության ցանցի անվտանգությանը՝ ֆայերվոլի (ցանցի պաշտպանիչ համակարգ) միջոցով, որը առաջին պաշտպանական գիծն է և վերահսկում է ներտիրույթային և արտաքին ցանցերի միջև տվյալների շարժը:

Քաղաքականություն

- **Ֆայերվոլի տեղադրում**. բոլոր համակարգիչները և ցանցային սարքերը պետք է ունենան ֆայերվոլ (ծրագրային կամ սարքային):
- **Ֆայերվոլի կարգավորում**. կարգավորում կատարողը պետք է լինի SS մասնագետ, որպեսզի թույլատրելի ու արգելված կապերը ճիշտ սահմանվեն:
- **Ցանցի պաշտպանություն**. ֆայերվոլը պետք է տեղակայված լինի ցանցային պարագծում՝ պաշտպանելով ներքին ցանցը:
- **Մուտքի կառավարում**. միայն նշանակված SS աշխատակիցները կարող են փոփոխել ֆայերվոլի կարգավորումները:
- **Տարեկան վերանայում**. տարեկան կամ ըստ փոփոխությունների, պետք է վերանայել firewall-ի կանոնները (rules):

Ինչպե՞ս կիրառել (How-To)

1. Windows-ում միացրեք «Windows Defender Firewall»-ը կամ այլ երրորդ կողմի ֆայերվոլ (third-party firewall): macOS-ում՝ այն ակտիվացրեք «Firewall» բաժնում
2. Կազմակերպչական մակարդակով (router-level firewall) օգտագործեք սարքային firewall/router, որտեղ կարգավորում եք արտոնված (allowed) և արգելված (blocked) պորտերը:
3. Գրանցեք «firewall change log»-ը, որպեսզի իմանաք՝ ով և երբ փոխեց «firewall»-ի կանոնները:

Գործնական օրինակ

- Եթե ձեր ներքին ցանցում ոչ ոք չի օգտվում FTP-ից (File Transfer Protocol/նիշքերի փոխանցման կանխագիր), ապա «firewall»-ում արգելեք 21 (FTP) պորտը, որպեսզի այն չհանդիսանա խոցելի բաց:

Լրացուցիչ ռեսուրսներ

- Անվճար «open-source firewall» լուծումներ – OPNsense կամ pfSense
- Ապարատային «router/firewall» – Ubiquiti EdgeRouter

---

11. Վեբկայքերի անվտանգություն

Նպատակ

Նպաստել կայքի տվյալների պաշտպանվածությանը կիբեռհարձակումներից (hack, DDoS, տվյալների արտահոսք) և մշտական հասանելիությանը:

Քաղաքականություն

- **SSL/TLS սերտիֆիկատ**. կայքի հասցեն պետք է սկսվի https://-ով:
- **Թարմացումների կառավարում**. CMS-ը (օրինակ՝ WordPress, Joomla, Drupal) և plugin-ներն անհրաժեշտ է պարբերաբար թարմացնել: Անվտանգության թարմացումները պետք է իրականացնել հնարավորինս արագ:
- **Մուտքի վերահսկում**. ադմին հաշիվների համար պետք է ակտիվացնել բազմափուլ վավերականացում (MFA), իսկ չգործածվող հաշիվները անմիջապես հեռացնել:
- **Պահուստավորում (Backup)**. առնվազն շաբաթական մեկ անգամ անհրաժեշտ է կատարել կայքի ամբողջական պահուստավորում:
- **SLA/Սպասարկում**. պետք է նախատեսել պայմանագիր (service level agreement) կայքը մշակող ընկերության կամ անհատի հետ՝ երկարաժամկետ անվտանգության մոնիտորինգի համար:
- **DDoS պաշտպանություն**. անհրաժեշտ է գործարկել DDoS պաշտպանությունն (օրինակ՝ Cloudflare, Project Shield, Deflect) ուղղված գործողություններ:

Ինչպե՞ս կիրառել (How-To)

1. Ստացեք անվճար SSL (օրինակ՝ Let's Encrypt), միացրեք HSTS, որպեսզի միշտ կիրառվի HTTPS տարբերակը:
2. WordPress-ում, Joomla-ում կամ այլ CMS-ում անջատեք «plugin»-ները, որոնք չեք օգտագործում: Անպայման թարմացրեք «core CMS»-ն ու «plugin»-ները:
3. Եթե երկարաժամկետ սպասարկման հնարավորություն չունեք, ապա օգտվեք «website builder»-ներից, որոնք ինքնուրույն կարգավորում են անվտանգության զգալի մասը և բավականին փոքր ամսավճարով ներառում սպասարկման ողջ փաթեթը:

Գործնական օրինակ

- Հասարակական կազմակերպությունները կարող են դիմել Cloudflare-ի «Galileo» ծրագրին միանալու և ստանալ անվճար DDoS պաշտպանություն:

Լրացուցիչ ռեսուրսներ

- Անվճար SSL/TLS սերտիֆիկատներ - Let's Encrypt
- Անվճար DDoS պաշտպանության ծրագրեր հասարակական կազմակերպությունների համար - Cloudflare Galileo / Project Shield

12. Պահուստավորում (Backup)

Նպատակ

Նպաստել տվյալների անվտանգ և ապահով կրկնօրինակմանը/պահուսատվորմանը՝ տվյալների և/կամ համակարգերի կորստի (կիբեռհարձակում, տեխնիկական վնաս) դեպքում դրանք վերականգնելու նպատակով։

Քաղաքականություն

- **Պարբերական պահուստավորում**. շաբաթական կտրվածքով անհրաժեշտ է կատարել պահուստավորում (backup), իսկ առանձնահատուկ կարևոր տվյալների դեպքում՝ ամենօրյա պահուստավորում։
- **Պահուստավորման վայրեր**. տվյալները պետք է պահուստավորել երկու կամ ավելի տարբեր վայրերում (տեղում/local և այլ տարածքում/off-site)։
- **Պահուստային տարածքի անվտանգություն**. արտացանցային (offline) կրիչները պետք է լինեն գաղտնագրված (encrypted), իսկ ամպային ծառայությունները՝ անվտանգ։
- **Վերականգնման փորձարկումներ**. առնվազն եռամսյակը մեկ անհրաժեշտ է փորձել վերականգնել տվյալները backup-ից, համոզվելու համար, որ այն իրականում աշխատում է։
- **Վերահսկում**. եթե backup-ը ինչ-որ պատճառով չի կատարվել, ապա պետք է տեղեկացնել/ահազանգել SS թիմին։

Ինչպե՞ս կիրառել (How-To)

1. Պետք է օգտագործել պահուստավորման ավտոմատ գործիքներ (օրինակ՝ Veeam, Acronis, Cobian Backup, RSYNC՝ Linux-ում)։
2. Պահեք պահուստային ֆայլերը երկու տեղ, օրինակ, ամպային միջավայրում (Dropbox, Google Drive, OneDrive) և արտաքին կրիչի վրա, որն ամեն օր համակարգին միացված չի մնում։

Գործնական օրինակ

- Պայմանական, կարող եք ամեն շաբաթ backup անել ամպային տարբերակում պահուստավորված տվյալները և ամեն ամիս offline կրիչինը։ Այսպես ransomware հարձակման դեպքում offline կրիչի վրա պահված ֆայլերը կմնան անվնաս։

Լրացուցիչ ռեսուրսներ

- Պահուսատվորման գործիք CLI open-source backup tool - Restic
- Linux/Mac-ում հաճախ օգտագործվող ֆայլերի համաժամացման/backup գործիք - Rsync

13. Տվյալների պահպանման քաղաքականություն (Data Retention Policy)

Նպատակ
Տվյալների պահպանման քաղաքականությունը սահմանում է կազմակերպությունում տվյալների պահպանման և անվտանգ վերացման կանոնները, նվազեցնում է տվյալների արտահոսքի և գաղտնիության խախտումների ռիսկերը, ինչպես նաև ապահովում է համապատասխանությունը անձնական տվյալների պաշտպանության կանոնակարգերին (օրինակ՝ GDPR, Անձնական տվյալների պաշտպանության մասին ՀՀ օրենք):

Քաղաքականություն

- **Տվյալների պահպանման նպատակի առկայություն**
    - Տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար:
    - Տվյալները պետք է պահպանվեն այն նվազագույն ժամկետով, որն անհրաժեշտ է տվյալների մշակման նպատակին հասնելու համար:
- **Պահպանման Ժամկետներ**
    - Կազմակերպությունը պետք է հստակ սահմանի, թե տվյալների որ տեսակներն ինչքան ժամանակ են պահպանվելու: Օրինակ՝ անձնական տվյալներ՝ առավելագույնը 1-3 տարի, ֆինանսական տվյալներ՝ 5-7 տարի:
    - Ժամկետի ավարտից հետո տվյալները պետք է ոչնչացվեն կամ անանունացվեն:
- **Տվյալների Վերահսկում**
    - Պահպանվող տվյալները պետք է պարբերաբար ստուգվեն և խմբավորվեն ըստ իրենց պահպանման ժամկետների:
    - Հստակեցրեք, թե ով է պատասխանատու տվյալների պահպանման ժամկետների վերահսկման համար:
- **Տվյալների Անվտանգ Վերացում**
    - Ժամկետն անցած տվյալները պետք է ոչնչացվեն այնպես, որ դրանք հնարավոր չլինի վերականգնել, այդ թվում՝ հնարավոր չլինի վերականգնել տեղեկատվական համակարգում առկա անձնական տվյալների բովանդակությունը: Սա ներառում է թվային ֆայլերի անվերադարձ ջնջումը հատուկ ծրագրերի միջոցով (secure deletion):
    - Թղթային փաստաթղթերը պետք է ոչնչացվեն շրեդերի միջոցով (shredding):
- **Պարբերական Վերանայում**
    - Պարբերաբար՝ տարեկան առնվազն մեկ անգամ, պետք է վերանայվեն տվյալների պահպանման ժամկետները, անհրաժեշտության դեպքում պետք է փոփոխություններ կատարել:
    - Վերանայման արդյունքում տվյալների մշակման նպատակներին հասնելու համար ոչ անհրաժեշտ անձնական տվյալներ հայտնաբերելու դեպքում

դրանք անհապաղ կամ նման հնարավորության բացակայության դեպքում երեք աշխատանքային օրվա ընթացքում պետք է ոչնչացվեն

- **Փաստաթղթավորում**
    - Տվյալների պահպանման և ոչնչացման բոլոր գործընթացները պետք է գրանցվեն փաստաթղթային կամ էլեկտրոնային եղանակով՝ ապահովելով դրանց հետագծելիությունը և վերահսկելիությունը:

Ահա տվյալների վերջնական (անվերականգնելի) ջնջման համար մի քանի վստահելի գործիքների տարբերակներ՝

Անվճար ծրագրեր՝

1. **Eraser** (Windows)
    - Հզոր, անվճար գործիք, որը կարողանում է պարբերաբար՝ նախապես տրված գրաֆիկով, անվերադարձ ջնջել տվյալները էլեկտրոնային կրիչներից:
    - https://eraser.heidi.ie/
2. **BleachBit** (Windows, MacOS, Linux)
    - Ազատ կոդով ծրագիր, որը հեռացնում է ֆայլերը՝ առանց վերականգնման հնարավորության:
    - https://www.bleachbit.org/
3. **File Shredder** (Windows)
    - Հեշտ օգտագործվող գործիք՝ մշտապես տվյալները ջնջելու համար:
    - https://www.fileshredder.org/
4. **CCleaner** (Windows, MacOS)
    - Լայնորեն տարածված ծրագիր, որը ներառում է ֆայլերի անվտանգության ջնջման հնարավորություններ:
    - https://www.ccleaner.com/

Այս գործիքները թույլ են տալիս ապահով կերպով ջնջել տվյալները՝ բացառելով հետագայում դրանց վերականգնման հնարավորությունը: Խորհուրդ է տրվում ընտրել գործիք, որը համապատասխանում է Ձեր կազմակերպության պահանջներին և տեխնիկական հնարավորություններին:

Լրացուցիչ գործողություններ թիրախավորված

կազմակերպությունների համար

Նպատակ
Նպաստել կազմակերպության պաշտպանվածությանը, երբ դրա որոշ ներկայացուցիչներ կարող են դառնալ թիրախավորված հարձակումների նպատակ (օրինակ՝ պետությունների կամ բարձրակարգ հաքերային խմբերի կողմից)։

Քաղաքականություն

- **Խորացված ուսուցում**. թիրախավորված անձինք (օրինակ՝ իրավապաշտպաններ, լրագրողներ) պետք է անցնեն առաջատար մակարդակի թվային անվտանգության վերապատրաստումներ

- **Խորացված մշտադիտարկում**. հնարավորության դեպքում պետք է թիմում ունենալ անվտանգության մասնագետ կամ մշտական կապ որևէ մասնագիտացված կազմակերպության հետ։

- **Հաշիվների խորացված պաշտպանություն**. կազմակերպության անդամները պետք է ակտիվացնեն խորացված հատուկ պաշտպանություն հաշիվների համար, որը տրամադրվում է էլեկտրոնային փոստի մատակարարների կողմից, օրինակ, Google Advanced Protection, Microsoft Account Guard, Proton Sentinel: Բոլոր հաշիվների վրա պետք է անջատվեն SMS-ների միջոցով վերականգնումը կամ բազմափուլային վավերացումը: MFA պետք է միացվի անվտանգության բանալիների (security key) միջոցով։

- **Լրտեսող ծրագրերի պաշտպանություն**. Թիրախավորված անձինք պետք է անցնեն վերապատրաստումներ հատուկ լրտեսական ծրագրերից պաշտպանվելու համար, ինչից հետո պետք է մշակել պաշտպանության հստակ ծրագիր՝ ցուցաբերելով պատշաճ հետևողականություն: Սա ենթադրում է, որ կազմակերպության ներկայացուցիչները պետք է հրաժարվեն հին հեռախոսներից, որոնք թույլ չեն տալիս ունենալ ամենաարդիական անվտանգության թարմացումները Android, iOS օպերացիոն համակարգերի համար: Գերադասելի է օգտագործել կա՛մ iPhone, կա՛մ Google Pixel հեռախոսներ։

- **Տեղեկատվության գաղտնագրում**. կազմակերպության տվյալները պետք է գաղտնագրվեն: Տեղեկատվության բաշխումը աշխատակիցների միջև պետք է լինի հստակ, տարանջատվի և արձանագրվի։

- **Սցենարների ստեղծում և վարժանքներ**. խորհուրդ է տրվում նախօրոք մշակել գործողությունների փաթեթ (playbook) ռիսկային դեպքերի համար և պարբերաբար անցկացնել վարժանքներ։

Վերանայում և համապատասխանություն

Կիբեռանվտանգության այս քաղաքականությունը պետք է **վերանայվի ամեն տարի** կամ անվտանգության միջադեպերի, ինչպես նաև կազմակերպությունում մեծ փոփոխությունների դեպքում: Բոլոր աշխատակիցները և ներգրավված կողմերը պարտավոր են ծանոթանալ և հետևել այս քաղաքականությանը: Քաղաքականությանը

չհետևելը կարող է հանգեցնել ներքին պատասխանատվության մեխանիզմների գործադրման կամ պայմանագրի լուծարման (կախված կազմակերպության կանոններից)։

Վերջաբան

Սույն քաղաքականությունը նպատակ ունի խթանել հասարակական կազմակերպությունների թվային բոլոր ակտիվների և ենթակառուցվածքների (տվյալներ, համակարգեր, ցանցեր) պաշտպանությանը, աշխատակիցների իրազեկվածությանը, և շարունակական կրթությանը։ Քաղաքականությունն ամենօրյա աշխատանքային գործիք է, որը պետք է պարբերաբար վերանայվի և հարմարեցվի առկա ռիսկերին ու ռեսուրսներին և արտացոլի կազմակերպության իրական կարիքները։

Հուշում. ամենամյա ընդհանուր ժողովի ժամանակ կազմակերպեք 15-20 րոպե տևողությամբ անդրադարձ-քննարկում ուղղված այս քաղաքականության մեջ արտացոլված ստանդարտներին, լսեք բոլորի առաջարկները, կատարեք անհրաժեշտ թարմացումներ և ապահովեք, որ աշխատակիցները ծանոթանան և ստորագրեն թարմացված փաստաթուղթը։

Փաստաթղթի վերջ