DOI: https://doi.org/10.36719/2663-4619/117/138-144

Ramazan Eyyubov
Odlar Yurdu Universiteti
Riyaziyyat üzrə fəlsəfə elmlər doktoru
https://orcid.org/0009-0003-0546-0188
eyyubov54@mail.ru
Kənan Cəfərov
Odlar Yurdu Universiteti
Magistrant
https://orcid.org/0009-0005-64861488
ceferovkenan36@gmail.com

Kibertəhlükəsizlikdə müdafiə strategiyalarının formalaşmasında rolu

Xülasə

Məqalədə kibertəhlükəsizlikdə insan faktorunun zəif və güclü tərəfləri təhlil olunur. Təlim və simulyasiya modelləri vasitəsilə işçilərin təhlükəsizlik biliklərinin artırılması imkanları araşdırılmış, Azərbaycandakı yerli şirkətlərin təcrübəsinə istinad edilmişdir. Nəticədə, insan faktoruna əsaslanan yanaşmaların kibertəhlükəsizlik strategiyalarında mühüm rol oynadığı qənaətinə gəlinmişdir. Bu məqalədə kibertəhlükəsizlikdə insan faktorunun rolu və onun effektiv təlim vasitəsilə inkişaf etdirilməsi təhlil olunmuşdur. İşçilərin texniki və davranış yönümlü biliklərinin artırılması üçün simulyasiya əsaslı təlim modellərinin — xüsusilə MITRE ATT&CK və Lockheed Martin Cyber Kill Chain — istifadəsi araşdırılmışdır. Phishing hücumlarının statistik artımı, yerli təşkilatların (SOCAR, Azercell və s.) yanaşmaları və təlimlərin mərhələli tətbiqi üzrə praktiki plan təqdim olunmuşdur. Məqalə kibertəhlükəsizliyin texnoloji yanaşmadan daha çox insan mərkəzli yanaşma ilə gücləndirilə biləcəyini göstərir.

Açar sözlər: *insan faktoru, kibertəhlükəsizlik, təlim, simulyasiya, hücum mərhələləri, Phishing, OPSEC*

Ramazan Eyyubov
Odlar Yurdu University
Doctor of philosophy in mathematics
https://orcid.org/0009-0003-0546-0188
eyyubov54@mail.ru
Kanan Jafarov
Odlar Yurdu University
Master student
https://orcid.org/0009-0005-64861488
ceferovkenan36@gmail.com

Role in Forming Defense Strategies in Cybersecurity

Abstract

The article analyzes the strengths and weaknesses of the human factor in cybersecurity. The possibilities of increasing employee security knowledge through training and simulation models are explored, and the experience of local companies in Azerbaijan is referenced. As a result, it is concluded that human factor-based approaches play an important role in cybersecurity strategies. This article analyzes the role of the human factor in cybersecurity and its development through effective training. The use of simulation-based training models-specifically MITRE ATT&CK and Lockheed Martin Cyber Kill Chain-to enhance employees' technical and behavioral knowledge is explored. The statistical increase in phishing attacks, the approaches of local organizations (SOCAR, Azercell, etc.),

and a practical plan for the phased implementation of training are presented. The article shows that cybersecurity can be strengthened with a more human-centric approach than a technological one.

Keywords: *Human factors, cybersecurity, training, simulation, attack phases, Phishing, OPSEC*

Giriş

Rəqəmsal texnologiyaların sürətli inkişafı kibertəhlükəsizliyi müasir təşkilatlar üçün strateji vacib sahəyə çevirib. Təşkilatlar və fərdi istifadəçilər üçün məlumatların qorunması kritik məsələdir. Texnoloji həllər artmaqla yanaşı, insan faktoru hələ də ən zəif həlqə kimi qalır. İnsan səhvləri, məlumatın düzgün idarə olunmaması və təhlükəsizlik qaydalarına əməl etməmək nəticəsində kiberhücumlar çox vaxt uğur qazanır. Bu səbəbdən, insan biliklərinin artırılması, təhlükəsizlik şüurunun formalaşdırılması və müntəzəm təlimlərin həyata keçirilməsi kibertəhlükəsizliyin təməl prinsiplərindən biridir.

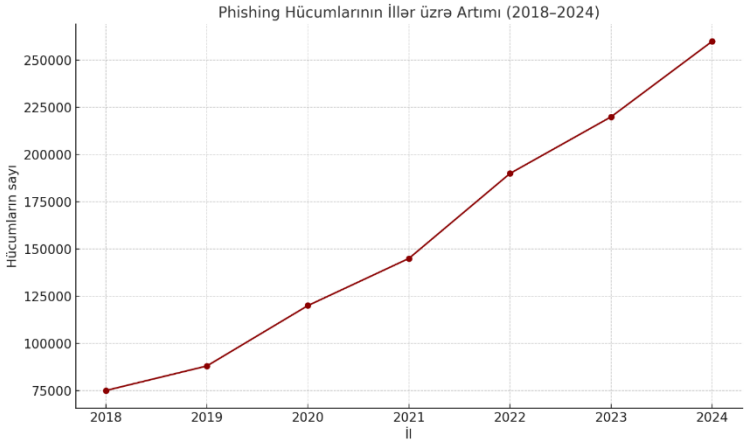
İnsan faktorunun kibertəhlükəsizlikdə yeri və önəmi. İnsanların təhlükəsizlik protokollarını düzgün tətbiq etməməsi, sosial mühəndislik hücumlarına qarşı həssas olmaları və ya sadəcə diqqətsizlikləri nəticəsində çox sayda kiberhücumlar baş verir. Phishing (saxta e-poçt və linklərlə məlumat oğurluğu), zəif və təkrar istifadə olunan parollar, icazəsiz proqram və cihazların istifadəsi (shadow IT), həmçinin təhlükəsizlik qaydalarının pozulması kimi hallar insan faktorunun yaratdığı ən geniş yayılmış risklərdir. Müxtəlif tədqiqatlara əsasən, informasiya təhlükəsizliyi insidentlərinin 90%-dən çoxu birbaşa insan amilindən qaynaqlanır ki, bu da insan faktorunun kritik zəiflik nöqtəsi olduğunu göstərir. Bu isə təsdiqləyir ki, texnoloji həllərdən əlavə, insan faktorunu idarə etmək önəmlidir.İnsan faktorunun zəiflikləri kibertəhlükəsizlikdə ən çox rast gəlinən təhlükələrdən biridir. Məsələn, 2023-cü ildə Microsoft-un apardığı tədqiqatlara əsasən, phishing hücumlarının böyük əksəriyyəti insan faktoruna – xüsusilə diqqətsizlik və məlumatlılığın azlığına – əsaslanır.

Phishing və sosial mühəndislikdə əsasn hədəflər, saxta mesajlar vasitəsilə etibarını qazanaraq şəxsi və maliyyə məlumatlarını itirə bilərlər. Misal üçün, 2020-ci ildə Facebook və Google böyük miqdarda pul vəsaitini phishing vasitəsilə itirmişdi.

Zəif Parollar, verizon hesabatına əsasən, zəif və təkrarlanan parollar şirkətlərdəki kiberinsidentlərin 80%-də iştirak edir. Parol siyasətinə əməl etməyən işçilər ciddi risklər yaradır.

İcazəsiz proqram və cihaz istifadəsi, IT bölməsinin nəzarətindən kənar texnologiyaların istifadəsi – yəni Shadow IT – təşkilatlarda məlumat axınının qeyri-rəsmi və nəzarətsiz şəkildə aparılmasına səbəb olaraq riskləri artırır. Gartner-in məlumatına görə, iş yerlərində istifadə olunan proqramların 30%-i IT departamenti tərəfindən təsdiqlənmir.

Yerli nümunəyə baxaq. Azərbaycanda fəaliyyət göstərən bəzi şirkətlərdə işçilərin şəxsi bulud saxlama hesablarından (məsələn, Google Drive, Dropbox) daxili sənədlərin göndərilməsi halları müşahidə olunmuşdur. Bu tip tətbiqlər Shadow IT-nin nümunəsidir və məlumatların üçüncü tərəfə nəzarətsiz şəkildə ötürülməsi ilə nəticələnə bilər. Belə hallar, daxili məlumat sızmasına və ya hüquqi pozuntulara yol açа bilər.



➤ **Şəkil 1.** 2018–2024-cü illər üzrə phishing hücumlarının artım dinamikası
(Mənbə: KnowBe4 Benchmarking Report, 2023)

Bu qrafik göstərir ki, hər il artan təhdid səviyyəsi kibertəhlükəsizlik sahəsində təlimlərin və preventiv tədbirlərin nə qədər vacib olduğunu bir daha sübut edir. Xüsusilə COVID-19 dövründə uzaqdan işləməyə keçidlə phishing riskləri daha da artmışdır.

Təlim və maarifləndirmənin kibertəhlükəsizlikdə roluna baxaq. Təlim proqramları işçilərin kibertəhlükəsizlik sahəsində məlumatlılığını artırmaq, təhlükəli vəziyyətlərdə düzgün davranış modellərini öyrətmək üçün hazırlanır. Təlimlərin effektivliyi isə test nəticələri, işçi davranışlarının monitorinqi, təhlükəsizlik hadisələrinin azalması və sorğular vasitəsilə ölçülür. Təlimlərin keyfiyyəti və davamlılığı təşkilatların ümumi kibertəhlükəsizlik səviyyəsini artırmaq üçün mühümdür.

Təlimlərin məqsədinin nədən ibarət olduğuna baxaq. İşçilərin kibertəhlükəsizlik riskləri barədə məlumatlılığını artırmaq və onların hücumlara qarşı düzgün reaksiya verməsini təmin etməkdir. Təlim proqramları müntəzəm olaraq yenilənməlidir.

Təlim əsas növlərini qeyd edək:Phishing simulyasiyaları KnowBe4 platformasında həyata keçirilir və işçilərin real hücumlara hazır olması təmin edilir.

1.Effektivlik ölçülməsi: Təlim nəticəsində phishing klikləmə faizi 60%-dən 15%-ə qədər azaldıla bilər **(KnowBe4 nəticələri)**.Təlimlərin planlaşdırılmasında yalnız texniki bacarıqlar deyil, həm də hüquqi və etik məsuliyyət sahələri nəzərə alınmalıdır. Xüsusilə şəxsi məlumatların qorunması, sistemlərə icazəli çıxış və təşkilat daxilindəki etik davranış kodeksləri hər bir təlim modulunun vacib hissəsi olmalıdır. Bu çərçivə həm yerli qanunvericilik, həm də beynəlxalq tələblər (GDPR, ISO/IEC 27001) üzrə formalaşdırılmalıdır.

2.Phishing hücumları və mübarizə təlimləri. Phishing, sosial mühəndislik hücumlarının ən geniş yayılmış formasıdır. Saxta e-poçtlar və ya vebsaytlar vasitəsilə istifadəçilərin şəxsi və maliyyə məlumatları ələ keçirilir. Hücumlar hədəfli (spear phishing), rəhbər şəxslərə yönəlik (whaling) və ya mövcud mesajların surəti şəklində (clone phishing) ola bilər. Bu hücumlara qarşı mübarizə üçün KnowBe4, Cofense kimi simulyasiya platformaları mövcuddur. Real vaxtda təşkil olunan phishing testləri işçilərin reaksiyasını qiymətləndirir və onların şüurunu artırır. Təlimlərdə təhlükəli linkləri və əlavələri tanımaq, təhlükəsiz hesabat vermək bacarıqları önə çıxarılır.

3.Phishing hücumlarına baxaq. 2022-ci il üzrə ABŞ-da qeydə alınmış kiberinsidentlərin təxminən üçdə biri, daha dəqiq desək 36%-i, fişinq hücumlarının nəticəsi olmuşdur (mənbə: KnowBe4 və ya Verizon). Spear phishing hədəfləri daha fərdiləşdirilmiş hücumlarla daha çox zərər görür. Əsas simulyasiya platformalarını qeyd edək. Cofense, PhishMe kimi alətlər istifadəçilərin hücumlara reaksiyasını qiymətləndirir və təlimlərin effektivliyini artırır.Praktiki tövsiyələr xüsusi yer tutur, İşçilərə e-poçtların göndəricisini diqqətlə yoxlamaq, linkləri birbaşa açmamaq, şübhəli faylları açmamaq və təhlükəsizlik komandasına dərhal məlumat vermək öyrədilməlidir. Güclü parol idarəetməsi və iki faktorlu autentifikasiya edilməsinə baxaq. Belə ki, parollar kibertəhlükəsizliyin əsas müdafiə xəttidir. Güclü parol siyasəti minimal uzunluq, müxtəlif simvolların istifadəsi, müntəzəm dəyişiklik və parolların təkrar olunmaması kimi prinsipləri ehtiva edir. Parol menecerləri (məsələn, LastPass, Bitwarden) istifadəçilərə təhlükəsiz və rahat parol idarəetməsi imkanı verir. İki faktorlu autentifikasiya (2FA) isə əlavə qoruyucu qat kimi, mobil tətbiqlər, SMS və ya fiziki cihazlar vasitəsilə istifadəçi identifikasiyasını gücləndirir. 2FA insan səhvlərinə qarşı effektiv qorunma yaradır və kiberhücumların qarşısını almaqda böyük rol oynayır. ABŞ-ın NIST standartları, parolların ən azı 12 simvoldan ibarət olması və unikal qaydada formalaşdırılmasını tövsiyə edir ki, bu da sistemlərin kompromisə uğramasının qarşısını alır.Bitwarden kimi açıq mənbəli proqramlar, həm şəxsi, həm də iş üçün təhlükəsiz parol idarəçiliyi təmin edir. İki faktorlu autentifikasiyanı izah edək. Google Authenticator istifadə edən şirkətlərdə hesab pozuntuları 80%-dən çox azalıb. Fiziki 2FA cihazları, məsələn YubiKey, ən yüksək təhlükəsizlik təmin edir.

4.Sosial mühəndislik hücumlarına qarşı təlim. Sosial mühəndislik hücumları insan psixologiyasından istifadə edərək təşkilatların təhlükəsizliyini zəiflətmək məqsədi daşıyır. Pretexting (yalan məlumatla etibara yiyələnmək), baiting (zərərli qurğular və ya cazibədar təkliflər), tailgating (icazəsiz fiziki giriş) kimi metodlarla hücumlar həyata keçirilir. Bu hücumlara qarşı təlimlərdə hücum metodlarının geniş izahı, real həyat nümunələri, praktiki məşqlər və rol oyunları vasitəsilə işçilərin şüuru artırılır.

Kiber Hücum Növlərinə baxaq. Tailgating hücumu fiziki təhlükəsizlik zəifliklərini göstərə bilər. Məsələn, böyük korporasiyalarda 15%-ə yaxın insidentlər bu yolla baş verir. İşçilərə real həyat nümunələri göstərilməli, rollu oyunlar vasitəsilə sosial mühəndislik hücumlarına qarşı davranış

bacarıqları formalaşdırılmalıdır. Kibertəhlükəsizlik sahəsində effektiv mühafizə yalnız texnoloji vasitələrlə deyil, həm də hücumların struktur və mərhələli gedişatını dərindən başa düşən işçi qüvvəsi ilə mümkündür. Bu məqsədlə **Cyber Kill Chain** və **MITRE ATT&CK** kimi strukturlaşdırılmış çərçivələrdən istifadə olunur. Bu modellər hücumların sistemli şəkildə öyrədilməsi və qarşısının alınması üçün nəzərdə tutulmuşdur. Təlim proqramlarında bu mərhələlərin simulyasiya yolu ilə praktiki şəkildə tətbiqi işçilərin təhlükəyə qarşı hazırlıqlı olmasını təmin edir və cavabvermə qabiliyyətini artırır.

Cyber kill chain modeli və onun təlimdə rolu. Lockheed Martin-in təqdim etdiyi Cyber Kill Chain çərçivəsi, hücum prosesini yeddi mərhələdə sistemləşdirərək hücumçunun davranışlarını analiz etməyə imkan verir. Hər mərhələ, hücumçunun məqsədinə çatmaq üçün atdığı konkret addımı ifadə edir. Bu mərhələlərin hər biri üzrə işçilərə müxtəlif növ hücum nümunələri göstərilir və uyğun müdafiə metodları öyrədilir:

1. **Kəşfiyyat (Reconnaissance):** Hücumçular hədəf təşkilat və ya şəxs haqqında açıq mənbələrdən (OSINT) məlumat toplayır.

•*Təlimdə öyrədilir:* Məlumatların onlayn məxfiliyi, sosial mediada ehtiyatlı davranış və "digital footprint" anlayışı.

• *Müdafiə strategiyası:* Open-source məlumatların azaldılması, DNS və WHOIS qeydlərinin məhdudlaşdırılması.

2. **Silahlandırma (Weaponization):** Hücumçu zərərli faylı (məsələn, PDF içindəki malware) yaradaraq onu çatdırmağa hazır vəziyyətə gətirir.

• *Təlimdə öyrədilir:* Fayl tipləri və zərərli əlavələrin identifikasiyası.

• *Müdafiə strategiyası:* Sandbox analizləri, SIEM ilə anomaliyaların aşkarlanması.

3. **Çatdırılma (Delivery):** Hücumçu zərərli faylı e-poçt, link və ya USB vasitəsilə hədəfə göndərir.

• *Təlimdə öyrədilir:* Phishing e-poçtlarının vizual analizi, URL-lərin yoxlanılması.

• *Müdafiə strategiyası:* E-poçt filtrasiya sistemləri, antivirus və anti-malware platformaları.

4. **İstismar (Exploitation):** Zəiflik vasitəsilə hücumçu sistemə giriş əldə edir.

• *Təlimdə öyrədilir:* CVE və exploit anlayışı, zəiflik aşkarlama testləri.

• *Müdafiə strategiyası:* Müntəzəm patch management, EDR sistemlərinin tətbiqi.

5. **Quraşdırma (Installation):** Hücumçu sistemə malware və ya backdoor qurur.

• *Təlimdə öyrədilir:* Uzaqdan idarə olunan alətlərin (RAT) fəaliyyəti.

• *Müdafiə strategiyası:* Endpoint Protection, davranış analizləri (UEBA).

6. **Əmr və nəzarət (Command and Control - C2):** Hücumçu ilə zərərli proqram arasında rabitə qurulur.

• *Təlimdə öyrədilir:* C2 serverlərin IP-ləri və domenləri ilə bağlı indikatorların tanınması.

• *Müdafiə strategiyası:* Network segmentation, DNS query monitorinqi.

7. **Məqsədin yerinə yetirilməsi (Actions on Objectives):** Məlumat oğurlanır, sistem pozulur və ya şifrələnir (ransomware).

•*Təlimdə öyrədilir:* Data exfiltration metodları, loqların yoxlanılması.

• *Müdafiə strategiyası:* DLP sistemləri, məlumatların şifrələnməsi, siqnalların izlənməsi.

MITRE ATT&CK modeli ilə təlim və müdafiəyə baxaq. MITRE ATT&CK

(Adversarial Tactics, Techniques & Common Knowledge) modeli daha geniş və təfərrüatlı struktur təqdim edir. O, hücumçuların istifadə etdiyi **taktika** və **texnikaları** konkret və real həyatda müşahidə edilmiş nümunələrlə təsvir edir. Təlimlərdə bu modeldən istifadə olunaraq işçilərə "real-case scenario"lar təqdim olunur və onlardan bu hücumları təhlil etmələri tələb olunur.

Məsələn:

- Taktika: **Initial Access**
- Texnika: **Spear Phishing Link**
- Müdafiə: Link analiz alətləri (VirusTotal, URLscan), DMARC/SPF siyasətləri.

Simulyasiya və hücum modelləri – IR Playbooks. Təlimlərin effektivliyini artırmaq məqsədilə Təhlükəsizlik Hadisələrinə Cavab Planları (Incident Response Playbooks) da hazırlanmalı və simulyasiya ilə tətbiq edilməlidir. Bu planlar müxtəlif hücum ssenarilərinə uyğun olaraq işçilərin və SOC komandalarının hansı addımları atmalı olduqlarını əvvəlcədən müəyyən edir. Məsələn, phishing hadisəsində ilkin cavab, hesabatlaşdırma, sistem yoxlaması və istifadəçi yönləndirməsi addım-addım

göstərilməlidir. İşçilər üçün hazırlanmış simulyasiya təlimləri, onların hücumları real vaxtda tanıma və düzgün cavab vermə bacarığını artırır. Bu ssenarilər aşağıdakı faydaları təmin edir:

- **Kritik düşünmə və analiz bacarığı** inkişaf etdirilir.
- **Təcili cavabvermə (Incident Response)** prosedurları praktiki tətbiq olunur.
- **Əməliyyat Təhlükəsizliyi (OPSEC)** vərdişləri formalaşır.

Məsələn:

- İşçiyə şübhəli bir e-poçt göstərilir → cavab reaksiyası ölçülür.
- Hücum mərhələsi ssenari üzrə izah olunur → qarşı tədbirlər seçilir.
- Zərərli hərəkətlər SIEM və ya EDR üzərindən təhlil olunur → məruzə hazırlanır.

Təhlükəsizlik mədəniyyəti və davamlı təlim olaraq, təşkilatlarda təhlükəsizlik mədəniyyətinin uğurla formalaşması rəhbərlik səviyyəsində nümunəvi davranışla birbaşa əlaqəlidir. CISO (Chief Information Security Officer), menecerlər və digər rəhbər şəxslər öz gündəlik fəaliyyətlərində təhlükəsizlik yanaşmalarına əməl etməklə, işçilər üçün motivasiyaedici model yaradırlar. Onların daimi dəstəyi və təhlükəsizlik mövzularında açıq kommunikasiya bu mədəniyyətin davamlılığını təmin edir. **Mədəniyyət:** Microsoft-da aparılan tədqiqat göstərdi ki, təhlükəsizlik mədəniyyətinin təşviq edildiyi müəssisələrdə kibertəhlükələrə qarşı hazırlıq səviyyəsi əhəmiyyətli dərəcədə yüksəkdir və insidentlərin sayı 50%-ə qədər azala bilər. **Davamlı Təlim:** Təlimlər interaktiv və motivasiyaedici olmalı, işçilərin iştirakını artırmaq üçün mükafatlandırma sistemləri tətbiq edilməlidir.

Azərbaycan bazarına dair nümunələr

- **SOCAR:** Kibertəhlükəsizlik strategiyalarında ISO/IEC 27001 standartlarına uyğunluq və ISMS həyata keçirilir. (SOCAR, 2024)

- **Azercell:** "Bug bounty" proqramları ilə təhlükəsizlik boşluqları aşkarlanır və SOC komandaları mütəmadi yenilənir. (Azercell, 2024)

- **Kapital Bank:** Davamlı phishing simulyasiyaları və MITRE ATT&CK modellərinə əsaslanan təhlil aparılır. (Kapital Bank, 2023)

Yerli şirkətlərin təcrübələri göstərir ki, davamlı təlim və simulyasiya strategiyaları informasiya təhlükəsizliyini artırmaqda əhəmiyyətli rol oynayır. Virtual Reallıq (VR) və Artırılmış Reallıq (AR) texnologiyalarının tətbiqi VR təlimləri real həyatı tam təqlid edən mühitlər yaratmaqla, kiberhücumların mərhələlərini praktik şəkildə öyrənməyə imkan verir. Artırılmış reallıq isə fiziki mühitdə zəifliklərin aşkar edilməsini və vizual təqdimatını təmin edir. Bu texnologiyalar təlimlərə yeni dinamizm gətirir, işçilərin diqqətini cəlb edir və öyrənməni dərinləşdirir. Cyberbit VR SOC Simulator kimi nümunələr bu sahədə uğurlu tətbiqlərdir. Cyberbit-in virtual reallıq simulyatorlarında iştirak etmiş işçilərin təhlükə mərhələlərini daha dəqiq tanımaq və cavab vermək qabiliyyətlərində 40%-ə qədər artım müşahidə edilmişdir. Fiziki mühitdə zəif nöqtələrin vizual olaraq göstərilməsi və işçilərin real vaxtda müdaxilə etməsi mümkündür.

İnsan davranışlarının psixoloji aspektləri və təhlükəsizlik əsas rol oynayır, belə ki insan psixologiyası kibertəhlükəsizliyin əsas elementlərindən biridir. İnsanlar çox vaxt emosional qərarlar verir, bu isə sosial mühəndislik hücumlarını daha təsirli edir. Məsələn, qorxu, təcili qərar vermə tələbi və ya maraq oyadan mesajlar istifadəçiləri yanlış kliklərə yönəldə bilər. Psixoloji manipulasiya faktorları – "authority bias", "urgency effect", və "scarcity principle" – sosial mühəndislik hücumlarında tez-tez istifadə olunur. Təlimlərdə bu psixoloji tələlərin izahı da verilməli, işçilər davranışlarında fərqindəlik səviyyələrini artırmalıdırlar.

Davranış analitikası və insan faktorunun monitorinqi müasir kibertəhlükəsizlik platformaları istifadəçi davranış analitikası (UEBA – User and Entity Behavior Analytics) vasitəsilə anormal davranışları aşkar edə bilir. Bu texnologiyalar insan faktorundan qaynaqlanan riskləri erkən mərhələdə müəyyən etməyə imkan verir.

Misal üçün bir istifadəçinin gecə saatlarında, xarici IP-dən birdən-birə çoxsaylı faylları yükləməsi anormal davranış sayılır və bu, potensial kompromis göstəricisi ola bilər.

Süni intellektə əsaslanan təlim platformaları işçilərin əvvəlki davranış və bilik səviyyəsinə uyğun fərdi təlim proqramları təklif edə bilir. Bu, təlimin effektivliyini artırır və resursların optimallaşdırılmasını təmin edir. AI əsaslı təlim sistemləri istifadəçinin zəif olduğu mövzular üzrə əlavə materiallar təqdim edir və onların bilik səviyyəsini adaptiv şəkildə inkişaf etdirir.

Təhlükəsizlik süurunun öyrənmə teoriyaları ilə əlaqələndirilməsinin öyrənmədə **Bloom taksonomiyası**, **Konstruktivizm** və **Kolb-un təcrübəyə əsaslanan öyrənmə modeli** kimi nəzəriyyələr tətbiq oluna bilər. Təlimlər yalnız informasiya ötürməkdən ibarət olmamalı, tətbiq, təhlil, sintez və qiymətləndirmə mərhələlərini də əhatə etməlidir.

Hüquqi və etik aspektlərə nəzər yetirək. Təşkilatlar yalnız texniki deyil, həm də etik və hüquqi məsuliyyət daşıyır. Təlimlərdə **Avropa İttifaqının Ümumi Məlumatların Qorunması Qaydaları (GDPR)**, **Azərbaycan Respublikasının "Şəxsi məlumatlar haqqında" qanunu**, **ISO/IEC 27001** və digər beynəlxalq normativ sənədlərə uyğun maarifləndirmə aparılmalıdır. İşçilər şəxsi məlumatların qorunmasının yalnız texniki deyil, **hüquqi və sosial məsuliyyət** daşıdığını da anlamalıdırlar. Etik baxımdan isə məlumatların icazəsiz istifadəsi, gizlilik pozuntuları və şəxsi maraqların təşkilat təhlükəsizliyi üzərində üstün tutulması ciddi pozuntu hesab olunur. Təşkilat daxilində etik davranış kodeksləri, məlumatlara çıxış səlahiyyətləri, və konfliktin qarşısının alınması siyasətləri tətbiq olunmalıdır.

İnsan faktorunun idarəsi yalnız mövcud işçilərin təlimindən ibarət deyil, həm də işə qəbul zamanı təhlükəsizlik şüuru və etik davranışa malik namizədlərin seçilməsi ilə başlayır. İşə qəbul prosesində psixometrik testlər və sosial mühəndislik ssenariləri ilə namizədin reaksiyası qiymətləndirilə bilər.

İnsan faktoru və təlimin gələcək perspektivlərinə nəzər salaq. Süni intellekt və avtomatlaşdırma təlimlərin fərdiləşdirilməsini və real vaxtda analizləri mümkün edir. Gamifikasiya (oyunlaşdırma) ilə təlimlər daha maraqlı və motivasiyaedici olur. Qlobal əməkdaşlıq və məlumat mübadiləsi isə təşkilatlar arasında təcrübə və təhlükəsizlik standartlarının inkişafına təkan verir. Bu yeniliklər kibertəhlükəsizlik təlimlərinin gələcəkdə daha effektiv və interaktiv olmasına zəmin yaradır:

1.Süni İntellekt: AI əsaslı adaptiv təlim sistemləri real vaxtda istifadəçi davranışını təhlil edərək fərdi öyrənmə proqramları təklif edir.

2.Gamifikasiya: Təlim proqramlarına oyun elementlərinin əlavə olunması işçilərin marağını artırır və təlim müddətini uzadır.

3.Qlobal Əməkdaşlıq: Təşkilatlar arasında təhlükəsizlik təcrübələrinin paylaşılması kibertəhlükəsizlik mühitinin gücləndirilməsinə kömək edir.

Praktik Tətbiq Planı.

Mərhələ	**Təsvir**	**Müddət**	**Qiymətləndirmə**
1. Hazırlıq	Hücum modellərinin seçimi və təlim ehtiyaclarının müəyyənləşdirilməsi	2 həftə	Risk analizi
2. Təlim	İşçilərə nəzəri və praktiki təlimlərin keçirilməsi	1 ay	Testlər və praktiki tapşırıqlar
3. Simulyasiya	Real hücum ssenarilərinin canlandırılması	2 həftə	Müşahidə və hesabat
4. Qiymətləndirmə	Effektivliyin ölçülməsi və boşluqların analizi	1 həftə	Təkmilləşdirmə tövsiyələri
5. Davamlılıq	Rüblük yeniləmə və əlavə təlimlərin təşkili	Davamlı	Geri bildirim və audit

► **Cədvəl 1.** Təlim mərhələləri üzrə praktik tətbiq planı *(Mənbə: Müəllifin araşdırması əsasında hazırlanmışdır)*

Nəticə

Tədqiqat göstərdi ki, insan faktoru kibertəhlükəsizliyin həm zəif nöqtəsi, həm də güclü müdafiə dayağı ola bilər. İşçilərin bilik və bacarıqlarının artırılması üçün simulyasiya əsaslı təlimlər, phishing testləri və hücum modellərinin tədrisi böyük əhəmiyyət daşıyır. MITRE ATT&CK və Cyber Kill Chain kimi strukturların tətbiqi kibertəhlükələrə qarşı hazırlığı gücləndirir.

Süni intellekt və gamifikasiya texnologiyalarından istifadə isə təlimin fərdiləşdirilməsi və motivasiyanın artırılmasına şərait yaradır. Yerli və qlobal təcrübələrin birləşdirilməsi təşkilatlarda daha güclü təhlükəsizlik mədəniyyətinin formalaşmasına imkan verir.

Beləliklə, insan faktorunun düzgün idarə olunması və davamlı maarifləndirmə kibertəhlükəsizliyin texniki tədbirlərlə yanaşı gücləndirilməsinin əsas şərtidir.

Ədəbiyyat

1. Verizon. (2023). *2023 Data Breach Investigations Report*. Retrieved from https://www.verizon.com/dbir/
2. Microsoft. (2023). *The Human Element of Cybersecurity*. Retrieved from https://www.microsoft.com/security
3. KnowBe4. (2022). *Phishing by Industry Benchmarking Report*. Retrieved from https://www.knowbe4.com
4. MITRE Corporation. (2023). *ATT&CK Framework*. Retrieved from https://attack.mitre.org
5. Lockheed Martin. (2023). *Cyber Kill Chain Model*. Retrieved from https://www.lockheedmartin.com
6. Gartner. (2022). *Shadow IT: Managing Risks and Maximizing Benefits*. Retrieved from https://www.gartner.com
7. International Organization for Standardization. (2022). *ISO/IEC 27001 — Information Security Management*. Retrieved from https://www.iso.org/isoiec-27001-information-security.html
8. Cyberbit. (2023). *Cyberbit VR SOC Simulator Overview*. Retrieved from https://www.cyberbit.com
9. SANS Institute. (2023). *Security Awareness Planning Kit*. Retrieved from https://www.sans.org
10. National Institute of Standards and Technology (NIST). (2022). *Special Publication 800-50: Building an IT Security Awareness and Training Program*. Retrieved from https://nvlpubs.nist.gov
11. European Union Agency for Cybersecurity (ENISA). (2023). *Cybersecurity Training and Awareness Raising*. Retrieved from https://www.enisa.europa.eu/publications
12. Cofense. (2022). *The State of Phishing Defense*. Retrieved from https://cofense.com
13. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Wiley.
14. SOCAR. (2024). *Kibertəhlükəsizlik İcmalı: Risklərin Azaldılması və İnfrastrukturun Qorunması Strategiyası*. Bakı: SOCAR Təhlükəsizlik Departamenti. Retrieved from https://www.socar.az
15. Azercell. (2024). *Cybersecurity Strategy and Awareness Programs Overview*. Retrieved from https://www.azercell.com
16. Kapital Bank. (2023). *Cybersecurity Awareness and MITRE ATT&CK Implementation*. Retrieved from https://www.kapitalbank.az