AXBOROT XAVFSIZLIGI VA KIBERXAVFSIZLIK: RAQAMLI DAVRNING ASOSIY TALABLARI

Sattorov N.O.
Toshkent shahar adliya boshqarmasi bosh mutaxassisi

Annotatsiya

Raqamli dunyo rivojlanishi bilan axborot xavfsizligi va kiberxavfsizlikning ahamiyati ortib bormoqda. Har bir tashkilot va shaxs o‘z ma’lumotlarini himoya qilishga, tahdidlardan qochishga va kiber hujumlarni oldini olishga harakat qilmoqda. Ushbu maqolada axborot xavfsizligi va kiberxavfsizlik tushunchalari, tahdidlar va ularni bartaraf etish choralarini ko‘rib chiqamiz.

Kalit so‘zlar: Axborot xavfsizligi, kiberxavfsizlik, zararli dasturlar, phishing, DDoS hujumlari, kuchli parollar, ikki faktorli autentifikatsiya (2FA), zaxiralash, tarmoq xavfsizligi, sun’iy intellekt.

Axborot xavfsizligi va kiberxavfsizlik: Tushunchalar

- **Axborot xavfsizligi**: Ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash jarayoni. Bu, shuningdek, axborotlarni zararlanishi yoki yo‘qolishidan himoya qilishni anglatadi.
- **Kiberxavfsizlik**: Axborotni va tizimlarni kiber tahdidlardan himoya qilishga qaratilgan strategiya va chora-tadbirlar to‘plami. Kiberxavfsizlik, shuningdek, tarmoq, dastur va qurilmalarni himoya qilishni o‘z ichiga oladi.

Tahdidlar

1. **Zararli Dasturlar**:
   - **Viruslar**: Dasturlarni va fayllarni zararlashga mo‘ljallangan.
   - **Trojanlar**: Foydalanuvchilardan ma’lumotlarni yig‘ish yoki tizimga kirish uchun ishlab chiqilgan dasturlar.

- **Shpion Dasturlar**: Foydalanuvchi faoliyatini kuzatish va shaxsiy ma’lumotlarni yig‘ish uchun ishlatiladi.

2. **Phishing**:

- Foydalanuvchilardan shaxsiy ma’lumotlarni olish uchun yolg‘on e-pochta yoki veb-saytlar yaratish.
- Kiber jinoyatchilar ko‘pincha mashhur brendlar nomidan soxta xatlar yuborishadi.

3. **DDoS Hujumlari**:

- Tarmoqdagi serverlarga ko‘p miqdorda so‘rovlar yuborish orqali ularni ishdan chiqarish.
- Buning natijasida tashkilotning xizmatlari to‘xtab qolishi mumkin.

4. **Ijtimoiy Muhitda Manipulyatsiya**:

- Foydalanuvchilarni aldash va ulardan ma’lumot olish uchun ijtimoiy muhitda manipulyatsiya qilish.

Axborotni Himoya Qilish Choralar

- **Kuchli Parollar**:
  - Murakkab parollar yaratish, ularni muntazam ravishda o‘zgartirish.
  - Ikki faktorli autentifikatsiya (2FA) yordamida qo‘shimcha himoya.
- **Antivirus Dasturlari**:
  - Zararli dasturlarni aniqlash va yo‘q qilish uchun antivirus dasturlarini yangilab turish.
- **Zaxiralash**:
  - Muhim ma’lumotlarni muntazam zaxiralash va bulutli xizmatlardan foydalanish.
- **Tarmoq Xavfsizligi**:
  - Tarmoqda xavfsizlik devorlarini (firewall) o‘rnatish va xavfsiz VPN xizmatlaridan foydalanish.

Ta’lim va Ongni Oshirish

- **Xodimlarni O‘qitish**:
  - Har bir xodim axborot xavfsizligi va kiberxavfsizlik asoslari haqida bilimga ega bo‘lishi zarur.
  - Real hayotdagi misollar asosida treninglar o‘tkazish.
- **Foydalanuvchilar uchun Ma’lumot Berish**:
  - Internetdan foydalanish qoidalari va xavf-xatarlar haqida ma’lumot berish.

Kelajakda Axborot va Kiber Xavfsizligi

- **Yangi Texnologiyalar**:
  - Sun’iy intellekt va mashinaviy o‘rganish yordamida kiber tahdidlarni oldini olish va aniqlashda foydalanish.
  - Blokcheyn texnologiyasi ma’lumotlar xavfsizligini ta’minlashda muhim rol o‘ynashi mumkin.
- **O‘zgaruvchan Tahdidlar**:
  - Kiber tahdidlar tez o‘zgarib bormoqda, shuning uchun doimiy monitoring va yangi strategiyalarni ishlab chiqish zarur.

Xulosa

Axborot xavfsizligi va kiberxavfsizlik har bir shaxs va tashkilot uchun zaruriy talablardir. Raqamli davrda tahdidlarga qarshi kurashishda bilim va texnologiyalarni rivojlantirish muhim ahamiyatga ega. Har birimiz o‘z ma’lumotlarimizni himoya qilish va kiber tahdidlardan saqlanish uchun mas’uliyatli bo‘lishimiz kerak.

Foydalanilgan Adabiyotlar

1. "Cybersecurity Essentials" – Cisco Networking Academy
2. "Information Security: Principles and Practice" – Mark Stamp
3. "The Web Application Hacker’s Handbook" – Dafydd Stuttard, Marcus Pinto
4. "Kaspersky Cybersecurity Glossary" – Kaspersky
5. "The Art of Deception: Controlling the Human Element of Security" – Kevin D. Mitnick
6. "Security Engineering: A Guide to Building Dependable Distributed Systems" – Ross

J. Anderson
7. Internet resurslari:
8. NIST Cybersecurity Framework – National Institute of Standards and Technology
9. OWASP (Open Web Application Security Project)
10. Jurnallar va maqolalar:
11. "Journal of Cybersecurity" – Kiberxavfsizlik sohasidagi yangi tadqiqotlar va tahlillarni yorituvchi ilmiy jurnallar.
12. "IEEE Security & Privacy" – Kiber xavfsizlik va axborot xavfsizligi bo‘yicha zamonaviy tadqiqotlar.
13. Sarvar o’g’li, M. S. (2024). DAVLAT BOSHQARUV TIZIMINING VA UNING MOXIYATI. Ta'limning zamonaviy transformatsiyasi, 8(4), 192-196.
14. Abdug'aniyev, B. (2020). Анализ инструментов расследования цифровой криминалистика. Архив Научных Публикаций JSPI.
15. Alishev, S. A., & Alishev, A. A. (2022). FORMATION OF STUDENTS'COMPETENCE TO OBTAIN INFORMATION USING INTERNET RESOURCES. In ТЕОРИЯ И ПРАКТИКА СОВРЕМЕННОЙ НАУКИ (pp. 128-130).