**IoT ulgamyna abanýan howplary ýüze çykarmak**

IoT ulgamyndaky enjamlar hem-de olaryň aragatnaşygy, köp görnüşli we dürli torlary öz içine alýar, şonuň üçin bu ulgamda ýüze çykyp biljek howplar we onuň alamatlaryny ýüze çykarmak has çylşyrymly bolup biler. Şuňa görä-de, IoT ulgamyny goramak, olara abanýan howplary ýüze çykarmak we öňüni almak üçin döwrebap tehnologiýalary we usullary ulanmak zerurdyr.

Bu ýerde biz IoT ulgamyndaky howplary ýüze çykarmak üçin ulanylýan usullar, tehnikalar we gurallar gürrüň ederis. Howplary düzgünli bir şekilde ýüze çykarmak, IoT ulgamynyň howpsuzlygyny üpjün etmäge we soňky netijede ulanyjylaryň hem-de ulgamyň özleriniň goraglylygyny üpjün etmäge kömek eder.

1. **IoT enjamlar üçin “Pentesting” synagy**

Pentesting — bu, tiz wagtda bir ulgamyň ýa-da enjamyň gorag ulgamynyň gowşak taraplaryny tapmak we olary barlamak üçin ýerine ýetirilýän synagydyr. IoT (Internet of Things) ulgamlarynda bu synaglar - enjamlarda we torlarda ýüze çykyp biljek howplary anyklamakda möhüm rol oýnaýar.

### ****Pentesting-iň maksady:****

* IoT enjamynyň ýa-da ulgamynyň goragynyň gowşaklyklaryny tapmak.
* Tor protokollaryndaky we enjamdaky zerur däl açyk portlary we hyzmatlary tapmak.
* Enjamlaryň arasynda geçirilýän maglumatlaryň goraglylygynyň derejesini ýüze çykarmak.
* Simli ýa-da simsiz torlardaky gowşaklyklar we hut bu ulgamlaryň arasynda bolup biljek hüjümleriň öňüni almak.

### ****Pentesting döwründe gözegçilik edilmeli elementler:****

* **Enjamyň fiziki goragy:** Enjamyň fiziki elýeterliligi, onuň şifrlenýän maglumatlaryna elýeterlilik
* **Protokollar we aragatnaşyk:** IoT enjamlar dürli protokollar (HTTP, MQTT, CoAP we ş.m.) bilen aragatnaşyk saklaýar. Bu protokollaryň gowşak taraplary tapylmalydyr.
* **Web we API interfeýsleri:** IoT enjamynyň web interfeýsi we API-ler arkaly giriş mümkinçiligi gözden geçirilmeli. Ýeňil parollar we maglumatlaryň açyk formatda iberilmegi ýaly gowşaklyklar tapylyp bilner.
* **Tor we açyk portlar:** Tor aragatnaşygyndaky portlaryň we hyzmatlaryň dogry sazlanýandygyny anyklamak.
* **Firmware we kod barlagy:** Enjamda ulanylan firmware-iň gowşaklyklaryny we öňden bellige alnan ýalňyşlyklary tapmak.

### ****Pentesting-iň usullary:****

* **Skanerler we port barlagy:** Nmap ýa-da Shodan ýaly gurallar bilen açyk portlary tapmak.
* **Düzgün bozulmalar(Exploitation):** Enjamda anyk gowşaklyklar tapylandan soň, olary peýdalanyp hüjüm etmek.
* **Brute force hüjümleri:** Ýeňil parollary tapmak we ulgama girmek üçin bu usul ulanylyp bilner.
* **API barlagy:** Enjamyň API interfeýsiniň goraglylygyny barlamak we onuň ýalňyyşlyklaryny ulanmak mümkinçilikleri.
* **Wi-Fi torlarynyň goragy:** Enjamyň Wi-Fi torunyň gorag derejesini we Wi-Fi parollarynyň güýçliligini barlamak.

### ****Pentesting-iň gurallary:****

* **Metasploit**
* **Burp Suite**
* **Wireshark**
* **Nessus**
* **Kali Linux bar bolan gurallar toplumy**

1. **Torlaryň işjeňligine gözegçilik etmek**

IoT ulgamynda torlaryň işjeňligine gözegçilik etmek, enjamlar we tor aragatnaşyklary bilen baglanyşykly howplary ýüze çykarmak üçin möhüm ädimdir. Torlygyň işjeňligi boýunça gözegçilik etmek, tordaky ähli maglumat alyş-çalyşygynyň we aragatnaşyklaryň analizi arkaly enjamlaryň arasynda ýa-da enjamlar bilen serwerleriň arasynda , olaryň torlarynyň arasynda bolup geçýän hereketleri yzarlamaga mümkinçilik berýär.

### ****Gözegçilik edilmeli elementler:****

* **Maglumat alyş-çalyşygy:** Enjamlaryň arasynda maglumatlar nädip iberilýär, nädip kabul edilýär we haýsy protokollar ulanylýar.
* **Enjamlaryň aragatnaşygy:** Tordaky dürli enjamlaryň arasynda bolup geçýän baglanyşyklar we olaryň hereketi.
* **Trafik we protokollar:** Tor üsti bilen iberilýän maglumatlaryň görnüşi (HTTP, MQTT, CoAP we ş.m.) we şifrlenme derejesi.
* **Tora düşýän agram:** Enjamlar ýa-da torlaryň arasynda degişli täsir we ýüz tutmalar (DDoS hüjümleri, gurnalan hereketler).

### ****Ýüze çykarylýan howplar:****

* Şifrlenmedik ýa-da açyk protokollaryň ulanylmagy, maglumatlaryň başga adamlara elýeterli bolmagyna sebäp bolup biler.
* Gözegçilik edilýän torlaryň netijesinde, DDoS hüjümleri, "man-in-the-middle" (MitM) hüjümleri we beýleki kiberhowplar ýüze çykyp biler.
* Torlaryň ýa-da enjamlaryň arasynda adaty däl trafikleriň bardygy.

### ****Gözegçilik gurallary:****

* **Wireshark**
* **Tcpdump**
* **Zeek (Bro)**

1. **IoT enjamlarynyň fiziki howpsuzlygynyň barlagy**

Kiberhowpsuzlyk bilen bilelikde, fiziki howpsuzlyk hem möhüm rol oýnaýar, sebäbi IoT enjamlary köplenç açyk giňişliklerde, ofislerde, zawodlarda, jaýlarda we transport ulgamlarynda ulanylýar. Fiziki taýdan goragsyz enjamlara kiberhüjümçiler aňsatlyk bilen fiziki aralaşma arkaly täsir edip bilerler. IoT enjamlary fiziki taýdan şu hüjümlere sezewar bolup biler:

### ****1. Fiziki elýeterlilik arkaly hüjümler****

* **Rugsatsyz elýeterlilik:** IoT enjamlary howpsuzlygy pes bolan ýerlerde ýerleşdirilende, bikanun adamlar olara fiziki taýdan täsir edip bilerler.
* **Enjamy fiziki taýdan bozmalar:** Hüjümçiler IoT enjamlarynyň içindäki komponentleri bozup ýa-da üýtgedip bilerler.
* **Modifikasiýa:** Enjamyň içki programmasyny (firmware) üýtgedip, ony zyýanly programmalar bilen çalyşmak howpy bar.

### ****2. Maglumatlaryň ogurlygy****

* **Has duýgur maglumatlaryň göçürilmegi:** IoT enjamlary birnäçe duýgur maglumatlary saklap biler (meselem, kamera ýazgylary, saglyk maglumatlary).
* **Maglumat saklanylýan media enjamlarynyň ogurlanmagy:** Sensorlar, maglumat saklaýjy çipler fiziki taýdan ogurlanyp bilner.

### ****3. Energiýa we elektrik üpjünçiligine hüjümler****

* **IoT enjamlarynyň elektrik togundan kesmek:** Hüjümçiler IoT enjamyny elektrik torundan aýryp ýa-da batareýasyny çykaryp, ony işlemez hala getirip bilerler.
* **Öçürip-ýakmak arkaly gowşaklyk döretmek:** Enjamy birnäçe gezek öçürip-ýakmak arkaly işini bozmaga synanyşyp bilerler.

### ****4. Fiziki enjam bilen aragatnaşyk edýän simleri we portlary ulanyp hüjüm etmek****

* **USB we seriýa portlary arkaly hüjüm:** Eger IoT enjamynda açyk USB ýa-da UART portlary bar bolsa, hüjümçiler bu portlar arkaly ony modifikasiýa edip bilerler.
* **Tor kabelleriniň kesilmegi ýa-da üýtgedilmegi:** Enjamy internete ýa-da içki toruna birikdirýän kabelleri kesmek arkaly, onuň işleýşine päsgel berip bilýärler.

**IoT enjamlarynyň fiziki taýdan goralmagy üçin birnäçe çäre görülmelidir:**

### **Fiziki elýeterliligi çäklendirmek**

### **Maglumatlary goramak**

### **Tok çeşmelerini goramak**

### **Fiziki hüjümleri anyklamak üçin howpsuzlyk mehanizmlerini ornaşdyrmak**

### **Portlary we interfeýsleri goramak**

Выявление угроз в IoT (Internet of Things) — это критически важный процесс для обеспечения безопасности устройств, сетей и данных. Вот основные методы и подходы, которые используются для обнаружения угроз в IoT-экосистеме:

**1. Мониторинг сетевой активности**

* **Анализ сетевого трафика (NTA – Network Traffic Analysis)**
  + Выявление аномалий в передаче данных (например, необычно высокий трафик, подозрительные IP-адреса).
  + Использование IDS/IPS (системы обнаружения и предотвращения вторжений) для IoT-устройств.
* **Анализ протоколов**
  + Проверка корректности использования MQTT, CoAP, Zigbee и других IoT-протоколов.

### ****4. Тестирование на проникновение (Pentesting)****

* **Атаки на устройства**
  + Проверка уязвимостей (например, перебор паролей, эксплуатация открытых портов).
* **Атаки на облачные сервисы IoT**
  + Тестирование API и веб-интерфейсов (OWASP IoT Top 10).

### ****6. Управление уязвимостями****

* **Сканирование CVE для IoT**
  + Мониторинг баз уязвимостей (например, **CVE**, **ICS-CERT**).
* **Проверка конфигураций**
  + Аудит настроек устройств на соответствие стандартам (например, **NIST IoT Security Guidelines**).

### ****6. Управление уязвимостями****

* **Сканирование CVE для IoT**
  + Мониторинг баз уязвимостей (например, **CVE**, **ICS-CERT**).
* **Проверка конфигураций**
  + Аудит настроек устройств на соответствие стандартам (например, **NIST IoT Security Guidelines**).

### ****8. Threat Intelligence для IoT****

* **Использование IoC (Indicators of Compromise)**
  + Анализ угроз на основе актуальных данных (например, списки вредоносных ботнетов вроде **Mirai**).
* **Подписка на IoT-угрозы**
  + Мониторинг специализированных платформ (например, **Nozomi Networks**, **Palo Alto IoT Security**).

### ****9. Физическая безопасность****

* **Защита от tampering**
  + Обнаружение вскрытия корпуса (например, датчики вскрытия в промышленных IoT-устройствах).
* **Антиклонирование чипов**
  + Использование защищенных микросхем (Secure Element, TPM).

### \*\*IoT-da ulanyş aktivligini gözegçilik etmek: usullar we guralar\*\*

IoT ulgamlarında köp sanly enjamlar (kamera, sensorlar, akylly enjamlary) ylalaşýar, bu bolsa olary hüjümlere açyk edýär. \*\*Tor aktivligini gözegçilik etmek\*\* hüjümleri anyklamaga, datany goramaga we ulgamyň işleýşini gözegçilik etmäge kömek edýär.

---

## \*\*1. Näme üçin IoT tor trafigini gözegçilik etmeli?\*\*

- \*\*Hüjümleri anyklamak\*\* (Mirai ýaly botnetler).

- \*\*Datanıň sızmagyny anyklamak\*\* (şübheli IP adreslere maglumat ibermek).

- \*\*Ulgamyň işleýşini gözegçilik etmek\*\* (kök trafik üýtgemeleri ýalňyşlyklary görkezýär).

- \*\*DDoS hüjümleriniň öňüni almak\*\* (IoT enjamlary köplenç hüjümler üçin ulanylýar).

---

## \*\*2. Esasy gözegçilik usullary\*\*

### \*\*🔍 2.1. Tor trafiginiň analizi (NTA – Network Traffic Analysis)\*\*

\*\*Nädip işleýär?\*\*

- Paketleri tutmak we analiz etmek (mysal üçin \*\*Wireshark\*\*, \*\*Zeek\*\*).

- Aňsatlyklary gözlemek:

- Bir enjamdan köp trafik.

- Şübheli IP adresler bilen aragatnaşyk (darknetden gelenler ýaly).

- Standart däl portlar (mysal üçin, IoT-da 23-nji portda Telnet – howp!).

\*\*Mysal:\*\*

Akylly kamera gözlänilmeýän bir şaýt Çindäki serwere maglumat iberýär → Belki ol çözülendir.

### \*\*🛡️ 2.2. Hüjümleri anyklamak üçin ulgamlar (IDS/IPS)\*\*

\*\*IDS (Intrusion Detection System)\*\* – diňe howplary anyklayar.

\*\*IPS (Intrusion Prevention System)\*\* – hüjümleri bloklaýar.

\*\*IoT üçin meşhur çözgütler:\*\*

- \*\*Suricata\*\* / \*\*Snort\*\* – trafigi analiz etmek (signatura we aňsatlyklar esasynda).

- \*\*Zeek (Bro)\*\* – skriptler bilen işleýän gözegçilik ulgamy.

\*\*Suricata üçin mysal düzgü:\*\*

```

alert tcp any any -> any 23 (msg:"Telnet Bruteforce Attempt"; flow:to\_server; content:"login"; nocase; threshold:type threshold, track by\_src, count 5, seconds 60; sid:1000001;)

```

\*(Telnet arkaly parol synanyşyklary barada duýduryş berýär)\*

### \*\*📊 2.3. IoT protokollaryny analiz etmek\*\*

IoT enjamlary özboluşly protokollary ulanyar: \*\*MQTT, CoAP, Zigbee, LoRaWAN\*\*.

\*\*Howplar:\*\*

- \*\*Şifrelenmedik MQTT\*\* → Maglumatlaryň ogurlanmagy.

- \*\*CoAP-daky aňsatlyklar\*\* → Enjamlara hüjüm etmek.

\*\*Nädip gözegçilik etmeli?\*\*

- \*\*Wireshark + filterler\*\* (mysal üçin, `coap && ip.src==192.168.1.100`).

- \*\*Aýratyn analizatorlar\*\* (mysal üçin, \*\*MQTT Spy\*\*).

\*\*Hüjüm mysaly:\*\*

Hüjümçi MQTT tema `home/camera/stream`-a ýazylýar we awtorizasiýasyz wideo alýar.

### \*\*🤖 2.4. Maşyn öwrenişi bilen aňsatlyklary anyklamak\*\*

\*\*Nädip işleýär?\*\*

1. \*\*Adaty trafik profilini\*\* döretmek.

2. \*\*ML-modeli\*\* (mysal üçin, \*\*Isolation Forest\*\*, \*\*LSTM\*\*) üýtgeşmeleri gözlemek.

\*\*Aňsatlyk mysallary:\*\*

- Temperatura sensoru sekuntda 1000 soraw iberýär.

- Akylly lampa başga bir ýurtdaky serwere birikmek isleýär.

\*\*Guralar:\*\*

- \*\*ELK Stack (Elasticsearch + Kibana)\*\* – aňsatlyklary görkezmek.

- \*\*Apache Kafka + ML-modelleri\*\* – real wagtda analiz.

---

## \*\*3. Amaly guralar\*\*

| \*\*Gural\*\* | \*\*Näme üçin?\*\* |

|----------------------|----------------------------------------|

| \*\*Wireshark\*\* | Paketleriň çuňňur analizi |

| \*\*Zeek (Bro)\*\* | Tor protokollaryny gözegçilik etmek |

| \*\*Suricata\*\* | Hüjümleri real wagtda anyklamak |

| \*\*MQTT Spy\*\* | MQTT trafigini analiz etmek |

| \*\*ELK Stack\*\* | Aňsatlyklary görkezmek we gözlemek |

---

## \*\*4. Hüjüm mysaly we ony nädip anyklamaly?\*\*

\*\*Ssenariý:\*\*

Hüjümçi akylly kamerany çözýär we ony DDoS hüjümi üçin ulanyr.

\*\*Nädip anyklamaly?\*\*

1. \*\*Giden trafigiň artmagy\*\* (kamera köp IP adreslere paket iberýär).

2. \*\*Adat däl birikmeler\*\* (tanalmagan domenler bilen aragatnaşyk).

3. \*\*IDS-iň işjeňleşmegi\*\* (mysal üçin, Suricata portlary skanirleýändigini anyklayar).

\*\*Çözgüt:\*\*

- \*\*IPS arkaly şübheli IP-ni bloklamak\*\*.

- Kamera üçin täzelenme ýüklemek.

---

## \*\*Netije\*\*

IoT-da tor aktivligini gözegçilik etmek:

✅ \*\*Trafik analizi\*\* (Wireshark, Zeek).

✅ \*\*IDS/IPS\*\* (Suricata, Snort).

✅ \*\*Protokollary barlamak\*\* (MQTT, CoAP).

✅ \*\*ML bilen aňsatlyklary anyklamak\*\* (Kibana, Kafka).

Gözegçiliksiz IoT enjamlary hüjümçiler üçin aňsat maksat bolup biler. \*\*Trafiki yzygiderli gözegçilik etmeli\*\* we \*\*awtomatik goranma ulgamyny gurmak\*\* zerur.

Eger aýratyn guralyň gurnalmagy barada sorag bolsa, soraw beriň! 🚀

### \*\*Мониторинг сетевой активности в IoT: методы и инструменты\*\*

В IoT-сетях множество устройств (камеры, датчики, умные приборы) постоянно обмениваются данными, что делает их уязвимыми для атак. \*\*Мониторинг сетевой активности\*\* помогает выявлять аномалии, предотвращать взломы и защищать данные.

---

## \*\*1. Зачем мониторить сетевой трафик в IoT?\*\*

- \*\*Обнаружение вторжений\*\* (например, ботнеты вроде Mirai).

- \*\*Выявление утечек данных\*\* (передача информации на подозрительные IP).

- \*\*Контроль за работоспособностью\*\* (неожиданные скачки трафика могут указывать на сбои).

- \*\*Предотвращение DDoS\*\* (IoT-устройства часто используются для атак).

---

## \*\*2. Основные методы мониторинга\*\*

### \*\*🔍 2.1. Анализ сетевого трафика (NTA – Network Traffic Analysis)\*\*

\*\*Как работает:\*\*

- Перехват и анализ пакетов (например, через \*\*Wireshark\*\*, \*\*Zeek\*\*).

- Поиск аномалий:

- Необычно высокий трафик с одного устройства.

- Связь с подозрительными IP (например, из даркнета).

- Нестандартные порты (например, Telnet на порту 23 в IoT — риск!).

\*\*Пример:\*\*

Умная камера внезапно начинает отправлять данные на сервер в Китае → Возможно, она скомпрометирована.

### \*\*🛡️ 2.2. Системы обнаружения вторжений (IDS/IPS)\*\*

\*\*IDS (Intrusion Detection System)\*\* – только обнаруживает угрозы.

\*\*IPS (Intrusion Prevention System)\*\* – блокирует атаки.

\*\*Популярные решения для IoT:\*\*

- \*\*Suricata\*\* / \*\*Snort\*\* – анализ трафика на основе сигнатур и аномалий.

- \*\*Zeek (Bro)\*\* – гибкий мониторинг с поддержкой скриптов.

\*\*Пример правила Suricata для IoT:\*\*

```

alert tcp any any -> any 23 (msg:"Telnet Bruteforce Attempt"; flow:to\_server; content:"login"; nocase; threshold:type threshold, track by\_src, count 5, seconds 60; sid:1000001;)

```

\*(Предупреждает о попытках перебора пароля по Telnet)\*

### \*\*📊 2.3. Анализ протоколов IoT\*\*

Устройства используют специфичные протоколы: \*\*MQTT, CoAP, Zigbee, LoRaWAN\*\*.

\*\*Риски:\*\*

- \*\*MQTT без шифрования\*\* → Перехват данных.

- \*\*CoAP с уязвимостями\*\* → Атаки на устройства.

\*\*Как мониторить?\*\*

- \*\*Wireshark + фильтры\*\* (например, `coap && ip.src==192.168.1.100`).

- \*\*Специализированные анализаторы\*\* (например, \*\*MQTT Spy\*\*).

\*\*Пример атаки:\*\*

Злоумышленник подписывается на топик MQTT `home/camera/stream` и получает видео без авторизации.

### \*\*🤖 2.4. Машинное обучение для обнаружения аномалий\*\*

\*\*Как работает:\*\*

1. Собирается \*\*базовый профиль\*\* нормального трафика.

2. ML-модель (например, \*\*Isolation Forest\*\*, \*\*LSTM\*\*) ищет отклонения.

\*\*Примеры аномалий:\*\*

- Датчик температуры вдруг отправляет 1000 запросов в секунду.

- Умная лампочка пытается подключиться к серверу в другой стране.

\*\*Инструменты:\*\*

- \*\*ELK Stack (Elasticsearch + Kibana)\*\* – визуализация аномалий.

- \*\*Apache Kafka + ML-модели\*\* – потоковый анализ.

---

## \*\*3. Практические инструменты\*\*

| \*\*Инструмент\*\* | \*\*Для чего?\*\* |

|----------------------|----------------------------------------|

| \*\*Wireshark\*\* | Глубокий анализ пакетов |

| \*\*Zeek (Bro)\*\* | Мониторинг сетевых протоколов |

| \*\*Suricata\*\* | Обнаружение атак в реальном времени |

| \*\*MQTT Spy\*\* | Анализ MQTT-трафика |

| \*\*ELK Stack\*\* | Визуализация и поиск аномалий |

---

## \*\*4. Пример атаки и как её обнаружить\*\*

\*\*Сценарий:\*\*

Злоумышленник взламывает умную камеру и использует её для DDoS-атаки.

\*\*Как обнаружить:\*\*

1. \*\*Рост исходящего трафика\*\* (камера начинает слать пакеты на множество IP).

2. \*\*Необычные соединения\*\* (подключение к странным доменам).

3. \*\*Срабатывание IDS\*\* (например, Suricata видит сканирование портов).

\*\*Решение:\*\*

- Заблокировать подозрительный IP через \*\*IPS\*\*.

- Обновить прошивку камеры.

---

## \*\*Вывод\*\*

Мониторинг сетевой активности в IoT — это:

✅ \*\*Анализ трафика\*\* (Wireshark, Zeek).

✅ \*\*IDS/IPS\*\* (Suricata, Snort).

✅ \*\*Проверка протоколов\*\* (MQTT, CoAP).

✅ \*\*ML для аномалий\*\* (Kibana, Kafka).

Без мониторинга IoT-устройства становятся легкой добычей для хакеров. Нужно \*\*постоянно отслеживать трафик\*\* и \*\*настраивать автоматические системы защиты\*\*.

Если нужны примеры настройки конкретного инструмента — спрашивайте! 🚀

### ****IoT enjamlarynda gowşaklyklary dolandyrmak****

**IoT (Internet of Things) ulgamlary** sanly we fiziki dünýäniň özara baglanyşykly bolmagyny üpjün edýän enjamlar toplumydyr. Bu ulgamlaryň howpsuzlygyny üpjün etmek üçin, olaryň **gowşak taraplaryny dolandyrmak** we mümkinçilik berýän howplary azaltmak örän möhüm meseleleriň biridir. Gowşaklyklary dolandyrmak, IoT enjamlarynyň işjeňligini we ygtybarlylygyny ýokarlandyrmak üçin edilýän çäreleriň we strategiýalaryň toplumydyr.

## **1. IoT enjamlarynda gowşaklyklar näme?**

Gowşaklyklar, kiberhüjümçiler tarapyndan ulanylyp bilinýän howpsuzlyk kemçilikleri bolup, IoT ulgamlarynda dürli görnüşlerde ýüze çykyp biler:

* **Fiziki gowşaklyklar:** Enjamyň fiziki taýdan çalt elýeterli bolmagy, degişli şahsyýetiň rugsatsyz onuň düzüwlerini üýtgedip bilmegi.
* **Düzgünleşdirilmedik aragatnaşyk:** IoT enjamlarynyň köpüsi maglumatlary kodlamazdan iberýär, bu bolsa aragatnaşyga üçünji taraplaryň goşulmagyna ýol açýar.
* **Güýçsiz ýa-da açyk parollar:** Köp IoT enjamlary öňünden kesgitlenen (default) ýa-da güýçsiz parollar bilen gelýär, bu bolsa olary aňsat hüjüme sezewar edýär.
* **Täzeleme (update) ýetmezçiligi:** IoT enjamlarynyň firmware-ini täzelenmezlik howpsuzlyk gowşaklyklarynyň dörän ýagdaýynda olaryň öňüni almaga mümkinçilik bermeýär.
* **Şebeke gowşaklyklary:** IoT enjamlary Wi-Fi ýa-da beýleki torlara birikdirilende, gowşak ýa-da şifrlenmedik aragatnaşyk ulansa, kiberhüjümler üçin amatly şert döredilýär.
* **Halkara standarlarynyň berjaý edilmezligi:** IoT enjamlarynyň käbiri halkara howpsuzlyk standartlaryna laýyk däl bolup biler, bu bolsa olaryň kiberhowp derejesini ýokarlandyrýar.

## **2. IoT gowşaklyklaryny dolandyrmak strategiýalary**

IoT enjamlarynda howpsuzlygy üpjün etmek we gowşaklyklary dolandyrmak üçin birnäçe möhüm strategiýa bar:

### ****2.1. Enjamyň howpsuzlyk synaglary****

IoT enjamlarynyň gowşaklyklaryny ýüze çykarmak we ýok etmek üçin howpsuzlyk synaglary (penetrasiýa synagy, zyňyndy synaglary we ş.m.) geçirilmelidir.

* **Penetrasiýa synagy (Pentesting):** Ulgamyň we enjamlaryň gowşak taraplaryny tapmak üçin test geçirilýär.
* **Zyňyndy synagy (Fuzz Testing):** Bu usul arkaly, enjama dürli görnüşli maglumatlar iberilip, olary nädogry işledýän ýagdaýlar kesgitlenýär.

### ****2.2. Firmware we programma üpjünçiliginiň (software) yzygiderli täzelenmegi****

IoT enjamlarynyň howpsuzlygyny saklamak üçin olaryň firmware-i we programma üpjünçiligi yzygiderli täzelenmelidir.

* **Awto-täzelenme (Auto-Update):** Enjamlar howpsuzlyk täzelenmelerini awtomatiki usulda kabul etmeli.
* **Firmware dolandyryş platformalary:** Enjamlaryň täzelenmelerini merkezi ulgam arkaly dolandyrmak ulgamy döredilmelidir.

### ****2.3. Güýçli parol we şahsyýet tassyklamak (Authentication)****

Enjamlaryň howpsuzlygyny güýçlendirmek üçin şu çäreler görülmelidir:

* **Öňden kesgitlenen (default) parollary üýtgetmek**
* **Iki derejeli autentifikasiýa (2FA) ulanmak**
* **Şifrlenen (encrypted) şahsyýet tassyklama ulgamlary** ulanmak

### ****2.4. IoT enjamlarynyň şifrlenmegi (Encryption)****

Maglumatlaryň howpsuzlyk derejesini ýokarlandyrmak üçin şifrleme (encryption) ulanylmalydyr.

* **AES-256** ýaly güýçli şifrleme algoritmleri ulanylmaly.
* **Transport Layer Security (TLS) we Secure Socket Layer (SSL)** ýaly howpsuzlyk protokollary bilen maglumatlaryň daşarky hüjümlerden goralmagy üpjün edilmelidir.

### ****2.5. Şebeke howpsuzlygyny üpjün etmek****

IoT enjamlarynyň birikýän torlarynyň howpsuzlygy üpjün edilmelidir.

* **Wi-Fi goragy:** Güýçli WPA3 şifrleme ulanylmaly.
* **VPN ulanmak:** IoT enjamlarynyň internet bilen goragly baglanyşygyny üpjün etmek üçin VPN ulgamlary ulanylmalydyr.
* **Firewally we IDS/IPS ulgamlary:** IoT enjamlarynyň torlara nädogry baglanyşyklaryny we howply traffikleri kesgitläp bilýän ulgamlary ulanmaly.

### ****2.6. IoT enjamlary üçin howpsuzlyk düzgünlerini we standartlaryny ulanmak****

IoT enjamlaryny öndürýän we ulanýan kompaniýalar halkara howpsuzlyk standartlaryny berjaý etmeli:

* **ISO/IEC 27001** – maglumat goragy we tor howpsuzlygy.
* **NIST (National Institute of Standards and Technology) IoT howpsuzlyk düzgünleri**
* **GDPR (Maglumat goragy düzgünnamasy) we beýleki maglumat goragy kanunlary**

## **3. IoT enjamlary üçin gowşaklyk dolandyryş gurallary**

Gowşaklyklary ýüze çykarmak we ýok etmek üçin dürli howpsuzlyk gurallary ulanylyp bilner:

* **Shodan** – açyk IoT enjamlary üçin skanerläp, açyk portlary we gowşaklyklary anyklaýan gural.
* **Nmap** – Tor enjamlarynyň we açyk portlarynyň skaneri.
* **Wireshark** – Şebeke traffiklerini barlamak we hüjümleri anyklamak üçin ulanylýan gural.
* **Metasploit** – Gowşaklyklary anyklamak we synag etmek üçin peýdalanylýan pentesting platformasy.
* **OWASP IoT Top 10** – IoT ulgamynda iň giň ýaýran gowşaklyklary görkezýän standart.

## **4. Netije**

IoT enjamlarynyň goragsyzlygy kiberhüjümler üçin uly howp döredýär. Gowşaklyklary dolandyrmak IoT enjamlarynyň we ulgamlarynyň howpsuzlygyny üpjün etmek üçin zerur bolup, şu aşakdaky çäreler bilen ýerine ýetirilmelidir:  
✅ **Enjamlaryň howpsuzlyk synaglaryny geçirmek**  
✅ **Firmware we programma üpjünçiligini täzeläp durmak**  
✅ **Güýçli parol we şahsyýet tassyklamak**  
✅ **Şifrleme tehnologiýalaryny ulanmak**  
✅ **Şebeke howpsuzlygyny üpjün etmek**  
✅ **IoT howpsuzlyk düzgünlerini berjaý etmek**

Şol çäreler ýerine ýetirilse, IoT enjamlarynyň howpsuzlygy ýokarlanyp, kiberhüjümleriň öňi alynar. IoT ulgamlaryny howpsuz ulanmak üçin gowşaklyklary dolandyrmak işjeň we yzygiderli geçirilmelidir.