Elektron Təhlükəsizlik Mərkəzi

Qaynar xətt: 1654
Email: reports@cert.az
Ünvan: Azərbaycan, Bakı, Droqal döngəsi, 702-ci məhəllə

İnformasiya təhlükəsizliyi insidentlərinin qarşısının alınması və nəticələrinin aradan qaldırılması üçün Elektron Təhlükəsizlik Mərkəzinin tövsiyələri

Elektron Təhlükəsizlik Mərkəzi baş verən və ya baş verə biləcək insidentlər haqqında müraicətləri, xəbərdarlıqları qəbul edir, aşağıdakı təhlükəsizlik insidentlərinin qarşısını alır və tövsiyələr verir:

- *Xidmətdən imtina (DoS, DDoS);*
- *İnternet resurslarına hücumlar;*
- *Ziyanverici proqram növlərinin yaradılması və yayılması;*
- *İnternet şəbəkəsində phishing;*
- *Virusların yayılması;*
- *Botnetlər və s.*

Vətəndaşların kompüter insidentləri haqqında maarifləndirilməsi məqsədi ilə Mərkəzimiz insidentlərin qarşısının alınması və nəticələrinin aradan qaldırılması üçün tədbirlər haqqında tövsiyyələr hazırlamışdır.

1. **Saytların oğurlanması insidentlərinin qarşısının alınması və nəticələrinin aradan qaldırılması tədbirləri:**

   - ***Şəbəkə administratorları və İnternet resursların sahibləri üçün:***
     - idarəetmə sistemlərinə giriş şifrələrinin mütəmadi olaraq dəyişdirilməsi (xüsusilə də, saytın idarə panelinə girişi olan əməkdaşlar işdən ayrıldıqda);
     - internetə qoşulmuş kompüterlərdə parolların saxlanmasının qadağan olunması;
     - saytla işləyən əməkdaşların sayta giriş səlahiyyətlərinin bölüşdürülməsi (məsələn, saytdakı məlumatları redaktə edən əməkdaşın yalnız redaktəyə giriş səlahiyyətinin mövcud olması);
     - antivirus proqramlarının və firewalların versiyasının yenilənməsi;

- server və saytları idarə edən əməkdaşların server, kommutasiya qurğuları və kompüterlərə fiziki girişinin məhdudlaşdırılması.

- ***İstifadəçilər üçün:***
  - antivirus proqramlarının bazasını daim yeniləmək, kompüterdə virusların olub-olmamasını periodik olaraq yoxlamaq;
  - verilənlər bazasının kopyalanmadan mühafizəsi;
  - əməliyyat sistemini, brouzerləri və digər proqram təminatlarını istehsalçıların rəsmi veb səhifəsindən mütəmadi şəkildə yeniləmək;
  - naməlum istifadəçilərdən faylları qəbul etməmək;
  - tanınmayan resurslara malik əlavələri (faylları) qəbul etməmək;
  - faylları endirərkən ehtiyatlı olmaq;
  - proqram təminatları endirdikdən sonra, quraşdırarkən yoxlamaq;
  - çatlarda və ya məktublarda mövcud olan spamlarla ehtiyatlı olmaq, hər linkə klikləməmək.

2. Ziyanverici proqramların yaranması və yayılması ilə bağlı insidentlərin qarşısının alınması və nəticələrinin aradan qaldırılması tədbirləri:

- ***Şəbəkə administratorları və İnternet resursların sahibləri üçün:***
  - antivirus proqramı quraşdırmaq və saytın ehtiyat surət (rezerv kopyasını) almağı unutmamaq şərtilə bütün faylları viruslardan yoxlamaq;
  - saytın yoluxma səbəbini aradan qaldırmaq;
  - antivirus proqramını daim yeniləmək, saytı periodik olaraq yoxlamaq;
  - firewall quraşdırmaq;
  - əməliyyat sistemini, brouzerləri və digər proqram təminatlarını istehsalçıların rəsmi veb səhifəsindən mütəmadi şəkildə yeniləmək;
  - naməlum istifadəçilərdən faylları qəbul etməmək;
  - tanınmayan resurslara malik əlavələri (faylları) qəbul etməmək;
  - faylları endirərkən ehtiyatlı olmaq;
  - proqram təminatları endirdikdən sonra, quraşdırarkən yoxlamaq;

- çatlarda və ya məktublarda mövcud olan spamlarla ehtiyatlı olmaq, hər linkə klikləməmək.
- mürəkkəb şifrələrdən istifadə etməklə bütün şifrələri mütəmadi olaraq dəyişmək: ftp, ssh, mysql, saytın cms parolları və s.

- ***İstifadəçilər üçün:***
  - antivirus proqramlarının bazasını daim yeniləmək, kompüterdə virusların olub-olmamasını periodik olaraq yoxlamaq;
  - verilənlər bazasının kopyalanmadan mühafizəsi;
  - əməliyyat sistemini, brouzerləri və digər proqram təminatlarını istehsalçıların rəsmi veb səhifəsindən mütəmadi şəkildə yeniləmək;
  - naməlum istifadəçilərdən faylları qəbul etməmək;
  - tanınmayan resurslara malik əlavələri (faylları) qəbul etməmək;
  - faylları endirərkən ehtiyatlı olmaq;
  - proqram təminatları endirdikdən sonra, quraşdırarkən yoxlamaq;
  - çatlarda və ya məktublarda mövcud olan spamlarla ehtiyatlı olmaq, hər linkə klikləməmək.

3. Phishing-in qarşısının alınması və nəticələrinin aradan qaldırılması tədbirləri:

- ***Şəbəkə administratorları və İnternet resursların sahibləri üçün:***
  - tərkibində phishing linklər mövcud olan səhifələri blok etmək, həmin linkləri silmək;
  - saytların sındırılmasının qarşısının alınması üçün tövsiyyələrə analoji tövsiyyələr.

- ***İstifadəçilər üçün:***
  - saytların URL-ünvanlarını yoxlamaq;
  - öz hesabınızı təsdiq etmənizi tələb edən məktub aldıqda, məktubu göndərənin e-poçt ünvanının qanuni olub olmadığına diqqət edin;
  - antivirus proqramlarının bazasını daim yeniləmək, kompüterdə virusların olub-olmamasını periodik olaraq yoxlamaq;
  - əməliyyat sistemini, brouzerləri və digər proqram təminatlarını istehsalçıların rəsmi veb səhifəsindən mütəmadi şəkildə yeniləmək;

- naməlum istifadəçilərdən faylları qəbul etməmək;
- tanınmayan resurslara malik əlavələri (faylları) qəbul etməmək;
- faylları endirərkən ehtiyatlı olmaq;
- proqram təminatları endirdikdən sonra, quraşdırarkən yoxlamaq;
- çatlarda və ya məktublarda mövcud olan spamlarla ehtiyatlı olmaq, hər linkə klikləməmək.

4. **Botnetlərin qarşısının alınması və nəticələrinin aradan qaldırılması tədbirləri:**
   - firewall quraşdırmaq;
   - əməliyyat sistemini, brouzerləri və digər proqram təminatlarını istehsalçıların rəsmi veb səhifəsindən mütəmadi şəkildə yeniləmək;
   - naməlum istifadəçilərdən faylları qəbul etməmək;
   - tanınmayan resurslara malik əlavələri (faylları) qəbul etməmək;
   - faylları endirərkən ehtiyatlı olmaq;
   - proqram təminatları endirdikdən sonra, quraşdırarkən yoxlamaq;
   - çatlarda və ya məktublarda mövcud olan spamlarla ehtiyatlı olmaq, hər linkə klikləməmək.
   - sizdən şəxsi hesab şifrənizi, login, bank hesab məlumatları və s. tələb edən mesajları gözardı edin. Ciddi sistemlər bucür məktublar yolamırlar. Bu cür hallar baş verdikdə, həmin sistemin texniki dəstək bölməsinə müraciət edin;
   - tanımadığınız şəxslərə şifrələrinizi verməyin;
   - telefon vasitəsilə, şəxsən və ya elektron poçt vasitəsilə heç kimə konfidensial informasiya verməyin;
   - hər hansı bir saytda qeydiyyatdan keçərkən və ya hər hansı formaya şəxsi məlumatlarınızı əlavə etməzdən əvvəl, bu məlumatların konfidensiallığının saxlanacağına əmin olun;
   - İnternet resurslarda ödəmə etdiyiniz zaman HTTPS rejimindən istifadə etməniz məsləhət görülür. Həmçinin, HTTPS rejimində olan saytın sertifikatını yoxlamaq lazımdır.

5. DDoS hücumların alınması və nəticələrinin aradan qaldırılması tədbirləri:

- ***Şəbəkə administratorları və İnternet resursların sahibləri üçün:***
  - hədəf sistemin loglarını əldə etmək;
  - logların analiz olunması. DoS və ya DdoS hücumların növlərinin təyin olunması;
  - təyin olunmuş portların və müəyyən protokolların bağlanması, spam mesajları ignore etmək üçün xüsusi qaydaların əlavə olunması, kanalın məhdudlaşdırılması metodlarının tətbiq olunması və s.;
  - DoS və DdoS hücumlarda iştirak edən IP ünvanların sahiblərinə və ya hosting provayderlərinə botnet insidentlərinin aradan qaldırılması və ya spam mesajlarının göndərilməsi barədə xəbərdarlıq etmək;
  - Hədəf resursun sahibinə bu tip insidentlərin qarşısının alınması və nəticələrinin aradan qaldırılması haqqında məsləhətlərin verilməsi (təşkilatın ümumi təhlükəsizlik siyasətini təkmilləşdirmək).