

MƏDİA RESURSLARININ XARİCİ TEXNOLOGİYALARDAN ASILILIĞI AZALDILMALIDIR

RƏQƏMSAL SUVERENLİYİ HİSS ETDİRƏN PROBLEM

“Cloudflare” xidmətlərində yaranan kütləvi nasazlıq ölkəmizin internet şəbəkəsində də ciddi problemlər yaratdı. Ekspertlərin qənaətinə, qlobal internet insidentləri zamanı lokal infrastrukturla işləyən sistemlər daha dayanıqlıdır.



AYGÜN ƏZİZ
aygunaziz@kaspi.az

Ötən günlərdə ölkədə fəaliyyət göstərən bir çox xəbər portalında ciddi texniki problemlər qeydə alındı. Məlumat görə, bu, qlobal internet infrastrukturunun aparıcı təminatçılarından biri olan “Cloudflare” xidmətlərində yaranan kütləvi nasazlıqla bağlı idi. Nəticədə, onlarla yerli xəbər saytına giriş çətinləşdi, bəzi hallarda isə istifadəçilər tamamilə bu resurslara daxil ola bilmədilər. Hətta bəzi dövlət saytları da bu qlobal problemə təsirləndi. Bu da informasiya təhlükəsizliyi məsələsini yenidən gündəmə gətirdi.

“CLOUDFLARE” MƏSƏLƏSİ KİMİ BAXMAQ YANLIŞ OLAR

Məsələ ilə bağlı açıqlama verən Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin baş idarə rəisinin müavini Tural Məmmədov bildirdi ki, noyabrın 18-də 9000-dən çox yerli saytın fəaliyyətinin dayanmasına bir “Cloudflare” məsələsi kimi baxmaq yanlış olar. Qurum rəsmisi vurğuladı ki, böyük potensiala malik olan şirkətlərin qarşılarına qoyacaqları məqsədlərdən biri yerli məhsulların yaradılması ilə rəqəmsal suverenliyimizə dəstək olmasıdır. Bu, həm də ölkə Prezidentinin informasiya təhlükəsizliyi ilə bağlı təsdiqlədiyi strategiya ilə də qarşıya qoyduğu əsas tapşırıqlardan biridir: “Yerli məhsulların yaradılmasının və rəqəmsal suverenliyin vacibliyini hiss etdik. Bu, xüsusilə özəl sektorun xaricdən asılılığına bariz nümunə idi. Fəaliyyəti dayanan resursların içində media resurslarının da xüsusi çəkisinin olması bizi informasiya müharibəsinə hazırlıq səviyyəmizi də diqqətdə saxlamalı olduğumuza bir işarədir. Aydındır ki, lokal mühafizə həlləri ucuz başa gəlmir. Lakin dövlətimizin apardığı uğurlu siyasətin davamı olaraq bizim də həyata keçirdiyimiz informasiya təhlükəsizliyi siyasətində lokal həllərə üstünlük vermək və mühafizəni maksimal şəkildə lokal təmin etmək prioritet istiqamətlərimizdəndir”.

Məlumdur ki, bu hadisədən bəzi dövlət

saytları üzvi ağ çıxdı. Buna səbəb isə, trafik xaricə daşınmaması idi. T.Məmmədovun sözlərinə görə, son 3 ildə bir sıra dövlət qurumlarında istifadə edilən “Cloudflare” kimi trafik xaricə daşınması halı dayandırılıb və mühafizəsi “AzStateNet” üzərindən təmin edilib: “Ümumilikdə son 3 ildə 457 dövlət obyektinin şəbəkə təminatı “AzStateNet” üzərinə keçirilərək lokal mühafizəsi təmin olunub. Bizim həyata keçirdiyimiz sözügedən mühafizə siyasəti sadəcə internet informasiya ehtiyatları ilə bağlı deyil, bu yanaşma eyni zamanda xüsusi dövlət rabitəsində də şamil olunur”.

“MİLLİ TEXNOLOGİYƏ EKOSİSTEM GÜCLƏNDİRİLMƏLİDİR”

Kibertəhlükəsizlik üzrə ekspert Mehman İsgəndərov “Kaspi” qəzetinə açıqlamasında bildirdi ki, son insidentdə dövlət saytları lokallaşdırılmış təhlükəsizlik və infrastruktur həlləri sayəsində minimal təsirlə fəaliyyət göstərdi: “Xarici servise tam etibar olunmadığı üçün onlar qlobal insidentlərdən praktiki olaraq təsirlənmədilər. Lokal WAF, DDoS qoruma sistemləri, dövlət şəbəkəsi və müstəqil DNS xidmətləri bu cür hallarda əsas dayanıqlılıq mənbəyidir və xidmətlərin fasiləsizliyini təmin edir. Rəqəmsal suverenliyi gücləndirmək üçün prioritet istiqamətlər milli təhlükəsizlik sistemlərinin yaradılması, milli data-mərkəzlərinin genişləndirilməsi, ölkədaxili bulud və identifikasiya sistemlərinin inkişafı, milli DNS və sertifikat mərkəzlərinin qurulması və xarici texnologiyalardan asılılığın azaldılmasıdır. Dövlət strategiyasının məqsədi xarici riskləri minimuma endirmək, kritik məlumat axınına ölkə daxilində təmin etmək və milli texnoloji ekosistemi gücləndirməkdir”.

XARİCİ TEXNOLOGİYADAN ASILILIĞI NECƏ DAYANDIRMALI?

Mütəxəssis bildirir ki, bu problemlərlə üzləşməmək üçün özəl sektor və media resurslarının xarici texnologiyalardan asılılığı azaldılmalıdır: “Özəl sektor və media resursları üçün tövsiyələr hibrid modelin tətbiqi, lokal CDN və WAF xidmətlərinə keçid, məlumatların ölkə daxilində saxlanması, daxili monitoring və insident cavab mexanizmlərinin gücləndirilməsidir. Bu tədbirlər qlobal insidentlər zamanı xidmətlərin dayanıqlılığını artırır və təhlükəsizlik risklərini minimuma endirir. “AzStateNet” və digər lokal şəbəkə həlləri dövlət saytları və kritik infrastruktur üçün təhlükəsiz məlumat mübadiləsi təmin edir, xarici təsirlərə qarşı dayanıqlılığı artırır, trafik monitoringini asanlaşdırır və qlobal kəsintilərdən qoruyur. Belə

lokal həllər həm kibertəhlükəsizlik, həm də xidmətlərin fasiləsizliyi baxımından ciddi üstünlük yaradır”.

DAVAMLİ DAYANIQLILIQ ÜÇÜN VACİB NÜANSLAR

Həmsöhbətimiz onu da vurğuladı ki, qlobal internet insidentləri zamanı lokal infrastrukturla işləyən sistemlər daha dayanıqlıdır: “Yerli DNS, bulud platformaları, dövlət şəbəkəsi və milli təhlükəsizlik xidmətlərinin proaktiv monitoringi xidmətlərin fasiləsizliyini təmin edir. Ehtiyat routing mexanizmləri, lokal CDN və təhlükəsizlik xidmətlərinin genişləndirilməsi, həmçinin dövlət və özəl sektor arasında məlumat mübadiləsinin gücləndirilməsi və milli insident cavab mərkəzlərinin inkişafı davamlı dayanıqlılıq üçün vacibdir”.



**Mehman
İsgəndərov**