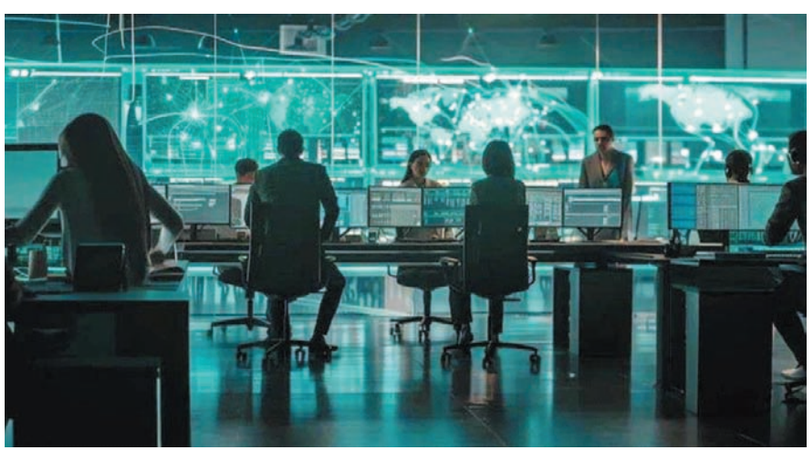
Kibertəhlükəsizlik artdıqca, zərərli giriş sorğusu bloklanır

Texnologiyanın sürətli inkişafı və rəqəmsallaşmanın həyatın hər sahəsinə inteqrasiyası ilə kibertəhlükəsizlik təkcə şirkətlər üçün deyil, həm də dövlətlər, fərdlər və bütövlükdə cəmiyyətlər üçün mühüm prioritetə çevrilib. Türkiyə də bu rəqəmsal transformasiya prosesində mühüm addımlar atır və kibertəhlükəsizlik sahəsində gələcəkdə daha çox diqqət yetirməli olduğu strategiyaları müəyyənləşdirir.

Türkiyə GDPR (General Data Protection Regulation) kimi Avropadakı qaydalara bənzər məlumatların qorunması qanunlarını tətbiq edir. 2019-cu ildə qüvvəyə minən Fərdi Məlumatların Qorunması Qanunu (KVKK) Türkiyədəki bizneslərdən kibertəhlükəsizlik siyasətlərini daha diqqətlə nəzərdən keçirmələrini tələb edir. Gələcəkdə kibertəhlükəsizlik sahəsində daha çox qaydalar və standartlar qurulacaq ki, bu da şirkətlərdən və hökumətdən kibertəhlükəsizlik strategiyalarını uyğunlaşdırmağı tələb edəcək.

Türkiyədə sənaye, ticarət, təhsil, səhiyyə və maliyyə sektorlarında da rəqəmsallaşma sürətlə davam edir. Bununla belə, bu transformasiya yeni kiber təhlükələri də yaradır. Xüsusilə IoT (əşyaların İnterneti) cihazlarının artması, bulud texnologiyalarının yayılması və süni intellekt proqramlarının tətbiqi casusların hədəf aldığı yeni sahələrdir. Bu da hökumətdən və özəl sektordan kibertəhlükəsizlik strategiyalarına daha çox sərmayə qoymağı tələb edir.

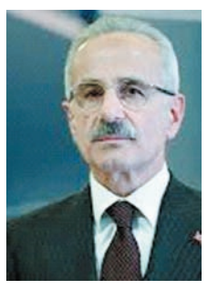
Süni intellekt (AI) kibertəhlükəsizlikdə inqilab etmək potensialına malik texnologiyalar kimi seçilir. Türkiyədə də bu sahəyə investisiyalar artır. Süni intellektlə işləyən kibertəhlükəsizlik hücumları daha tez aşkarlaya, şübhəli fəaliyyəti təhlil edə və potensial təhlükələrə qarşı müdafiə vasitələri inkişaf etdirə bilir. Süni intellektə əsaslanan həllər, xüsusilə kritik infrastrukturlara, hücumlara qarşı müdafiə mexanizmlərini gücləndirə bilir. Bu sahədə yerli proqram təminatının hazırlanmasına və süni intellekt tətbiqlərinə artan tələbat Türkiyənin kibertəhlükəsizlik sahəsində yerli potensialını daha da artıracaq. Türkiyə, beləliklə kibertəhlükəsizlik sahəsində dövlət tərəfindən dəstəklənən güclü infrastrukturu inkişaf etdirməyə davam edir. Kibertəhlükəsizlik sahəsində strateji investisiyalar və dövlət qurumları arasında əməkdaşlıq, ölkəni kiber təhdidlərə qarşı daha dayanıqlı edəcək. Kibertəhlükəsizlik mərkəzlərinin yaradılması, milli proqram təminatının inkişafı və kritik infrastrukturların təhlükəsizliyi istiqamətində aparılan işlər ölkənin bu sahədə müqavimətini artırır. Xüsusilə Prezidentin Rəqəmsal Transformasiya İdarəsi kibertəhlükəsizlik strategiyalarının yaradılması və həyata keçirilməsində mühüm rol oynayır.



Kibertəhlükəsizlik təkcə texniki deyil, həm də sosial məsuliyyət kimi həll edilməli olan bir məsələdir. Son illərdə ölkədə kibertəhlükəsizlik təhsili və məlumatlılığı da artır. Universitetlər, özəl sektorun təhsil müəssisələri və müxtəlif dövlət qurumları kibertəhlükəsizlik üzrə təlimlər keçirirlər. Bundan əlavə, ictimai məlumatlılığın artırılması və fərdlərin kibertəhlükəsizliklə bağlı məlumatlılığının artırılması böyük əhəmiyyət kəsb edir. Gələcəkdə kibertəhlükəsizlik üzrə təlimlərin daha da geniş vüsət alacağı və bütün səviyyəli istifadəçilər üçün müraciət edəcəyi gözlənilir. Həmçinin kibertəhlükəsizlik sahəsində beynəlxalq əməkdaşlığı gücləndirərək qlobal təhdidlərin öhdəsindən gəlməyi hədəfləyir. NATO və digər beynəlxalq təşkilatlarla əməkdaşlıq ölkəyə qlobal səviyyədə kibertəhlükəsizlik strategiyalarını möhkəmləndirməyə kömək edir. Bu əməkdaşlıq sayəsində kibercinayətkarlara qarşı daha effektiv mübarizə aparılır.

Türkiyədə kibertəhlükəsizlik rəqəmsallaşma tempinə paralel olaraq mühüm gündəm olmağa davam edir. Süni intellekt, dövlət tərəfindən dəstəklənən infrastruktur, təhsil və maarifləndirmə səyləri gələcək kibertəhlükəsizlik strategiyalarının təməl daşlarını təşkil edir. Türkiyə bu sahədə investisiyalarını artıraraq kiberhücumlara qarşı daha dayanıqlı bir cəmiyyət və iqtisadiyyat qurmağı planlaşdırır. Rəqəmsallaşma prosesində kibertəhlükəsizliyə məhəl qoymamaq böyük təhlükələrə və iqtisadi itkilərə də səbəb ola bilər. Buna görə də güclü kibertəhlükəsizlik infrastrukturunun yaradılması təkcə dövlətin deyil, həm də bütün sektorların və şəxslərin birgə məsuliyyətidir.

Onu da qeyd edək ki, Türkiyədə yanvar ayında Kiber Hadisələrə Müdaxilə Qrupları (SOME) tərəfindən 1,5 milyon İP ünvanına ümumilikdə 1 milyard 98 milyon 721 min 827 giriş sorğusunun bloklandığı bildirilir. Bu uğurlu müdaxilə ilə Türkiyənin kiber təhlükəsizliyi sahəsində əhəmiyyətli bir addım atılıb.



Bununla bağlı açıqlamanı **nəqliyyat və infrastruktur naziri Abdulkadir Uraloğlu** verib və Milli Kiber İnsidentlərə Müdaxilə Mərkəzinin (USOM) kibertəhlükələrin qarşısını almaq üçün fəaliyyətini fasiləsiz olaraq davam etdirdiyini bildirib. O, mərkəzin kiber insidentlərə cavab vermək, milli təhlükəsizlik və koordinasiyanı təmin etmək kimi mühüm vəzifələr daşıdığını vurğulayıb. Nazir deyib: "USOM yerli və xarici kiber təhdidlərin qarşısının alınması məqsədilə həyəcan siqnalları, xəbərdarlıq və elanlarla bağlı fəaliyyətlər həyata keçirir və kiber potensialın artırılması, texnoloji tədbirlər, təhlükə kəşfiyyatı və kritik infrastrukturların qorunması xidmətləri ilə Türkiyənin kiber təhlükəsizliyini təmin edir. USOM çərçivəsində, ölkəmizin kiber məkanı 2324 qrup və 8009 mütəxəssis heyəti ilə günün 24 saatı qorunur. 17 milyon IP ünvanı anında skan edilir və bu skanlarla proaktiv olaraq zəifliklər müəyyən olunur. 2025-ci ilin ilk ayında aparılan skanlarda 1165, bu günə qədər isə ümumilikdə 78558 kibertəhlükəsizlik aşkar edilib və müvafiq qurumlara məlumat verilib".

USOM-un 2013-cü ildən bu yana ümumilikdə 437.027 zərərli proqram və kiber hücum əlaqəsi aşkarladığını və bu əlaqələrə girişin bloklandığı bildirilib.

Nazir yerli və milli proqramlardan istifadə edilərək kiber insidentlərə qarşı mühüm addımlar atıldığını da bildirib. O, xüsusilə "Avcı", "Azad" və "Kasırga" kimi layihələrin milli kibertəhlükəsizliyə böyük töhfələr verdiyini vurğulayıb. Qeyd edib ki, USOM-un inkişaf etdirdiyi süni intellekt texnologiyası ilə yanvar ayında vətəndaşları aldatmağa yönəlmiş fişinq hücumları həyata keçirən 991 domen adına giriş bloklanıb və 5869 fişinq hücumunun qarşısı alınıb.

A.Uraloğlu son olaraq vurğulayıb ki, indiyədək SOME tərəfindən 1,5 milyon IP ünvanına edilən zərərli giriş sorğuları bloklanıb və bu prosesdə Türkiyənin kiber müdafiəsi gücləndirilib.

Esmira YAZKAN ASLANOVA,
"Respublika" qəzetinin
Türkiyə üzrə müxbiri.