ELEKTRON POÇT SERVİSİNDƏN İSTİFADƏ OLUNMASI İLƏ YARANAN RİSKLƏR

Əli Tağıyev,

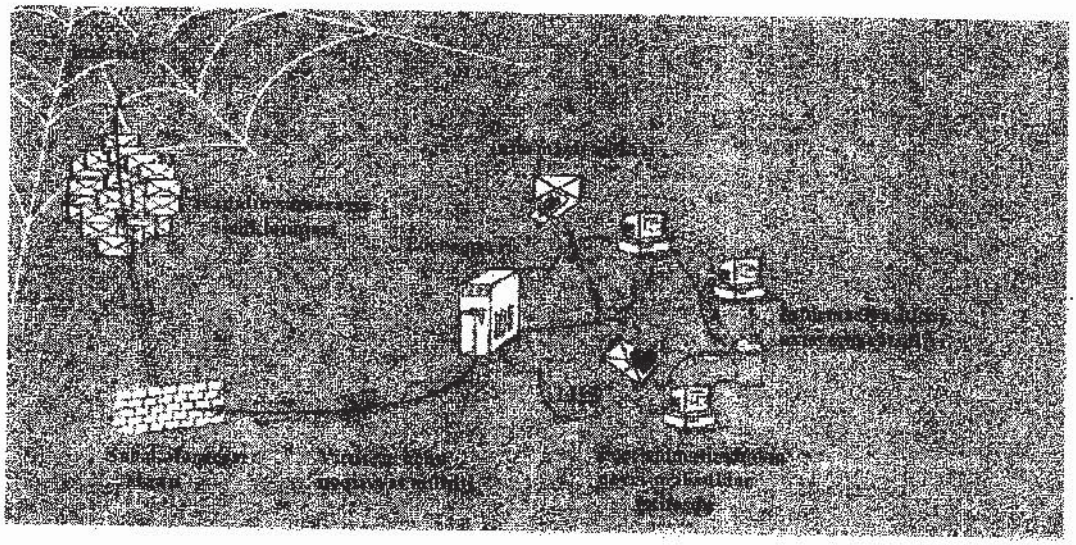
Ramin Hüseynov,
Azərbaycan Texniki Universiteti

Açar sözlər: elektron poçt, MIME standartı, şəbəkələrarası ekran, poçt serveri, informasiya itkisi, informasiya axtarışı, aralıq poçt serveri, resursların korlanması, elektron poçt arxivi, poçt müştərisi, bütövlük, adekvatlıq.

Elektron poçt çoxsaylı üstünlüklərə malikdir, lakin onun istifadə olunması ilə bağlı, məhz bu üstünlüklər səbəbindən əsas risklər yaranır. Məsələn, elektron poçtun hamı üçün əlçatan olması, onun bəzi üstünlüklərini çatışmazlıqlara çevirir, çünki istifadəsinin asanlığı və nəzarətsizlik informasiyanın sızmasına, müxtəlif formatlı sənədlərin ötürülməsi isə virusların yayılmasına səbəb ola bilər.

Nəticə etibarı ilə istənilən bu risklərdən biri şirkət üşün ciddi fəsadlar törədə bilər. Bu isə iş effektivliyinin itirilməsi, informasiyalı sistemlərin xidmət keyfiyyətinin aşağı düşməsi, informasiyanın məxfiliyinin itirilməsinə səbəb ola bilər. Bu problemə ciddi fikir verilməməsi biznes gəlirlərinin nəzərə çarpacaq dərəcədə azalmasına, bəzi hallarda isə qanunvericiliyin pozulmasına görə cinayət məsuliyyətinə cəlb olunmağa gətirib çıxarır.

MIME (*Multipurpose Internet Mail Extensions (elektron poçt xidmətinin çoxaspektli protokolu)*) standartının tətbiqi ilə əlaqədar olaraq, elektron poçtla müxtəlif formatlı böyük həcmli informasiyaların mübadiləsini təşkil etmək mümkündür. Bu imkandan cinayətkarlar dərhal istifadə etməyə başladılar, çünki, onlar bu informasiyalarla yanaşı istədikləri virusları yaya bilirlər. Elektron poçtun üstünlükləri artıq təhlükəyə çevirilir. Belə ki, elektron poçt istənilən bəd niyyətli informasiyaların, o cümlədən kompyüter viruslarının yayılması üçün ideal mühüt rolunu oynayır. Əgər elektron poçt üzərində lazımi nəzarət təmin olunmazsa, bu ciddi fəsadlara səbəb olar, hətta aradan qaldırıla bilməyən ziyanlar vura bilər. Bu cür risklərlə qarşılaşmamaq üçün "təhlükəli" məktubları blakirovka etmək və ya faylları antivirusla yoxlamaq olar. Təcrübədə müəyyən növ faylların blakirovka olunması daha optimal vasitə hesab olunur. Bunlar bir qayda olaraq exe., com., bat. fayllarıdır.



Şəkil 1. Mühafizə olunmayan poçt sisteminə müxtəlif faktorların neqativ təsiri.

Korparativ şəbəkələr üçün ciddi təhlükə elektron poçtun "korlanması" ilə bağlı olan müxtəlif növlü hücumlardır. Bu ilk növbədə böyük həcmli elektron poçt məlumatlarının göndərilməsi və faylların çoxdəfəli arxivləşdirilməsi ilə bağlıdır. Bu faylların və arxivlərin açılmasına cəht sistemin "donmasına" səbəb ola bilər. Bu zaman həm "xidmətdən imtina", "poçt bombaları" kimi planlaşdırılmış hücumlar, həm də planlaşdırılmayan hücumlar eyni dərəcədə təhlükəlidir.

Elektron poçtun digər xüsusiyyəti onun hamı üçün əlçatan və istifadəsinin sadəliyidir. Buna, bu növ İnternet xidmətinin geniş surətdə tətbiqi və istifadə olunası səbəb olmuşdur. Sürətli inkişaf və poçt servisinin fəaliyyətində vahid qaydaların olmaması nəzarət olunmayan elektron poçtun istifadə olunmasına, bununla bağlı bir çox risklərin yaranmasına gətirib çıxarmışdır.

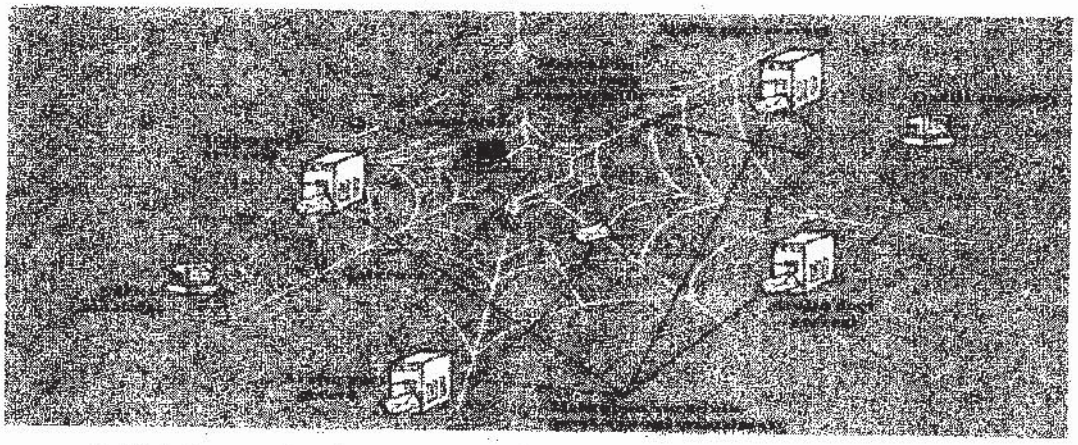
Poçt məlumatları üzərində nəzarətin olmaması, şirkət əməkdaşlarının elektron poçtdan şirkətin fəaliyyəti ilə bağlı deyil, digər məqsədlər (video-faylların və qrafikaların mübadiləsi, şəxsi yazışmalar, şirkətin poçt resurslarından istifadə etməklə öz bizneslərinin yaradılması və s.) üçün istifadəsinə səbəb olur. Bu isə bütünlükdə şirkət üzrə əmək məhsuldarlığının aşağı düşməsinə səbəb olur, çünki, əməkdaşların bu cür fəaliyyəti aşağıdakı fəsadların yaranmasına gətirib çıxarır:

- informasiya sisteminin işinin məhsuldarlığının azalması (qeyri-iş trafikinin həcminin artması);
- ayrı-ayrı əməkdaşların işinin məhsuldarlığının azalması (iş vaxtının səmərəsiz itkisi);
- informasiya sistemi resurslarının "korlanması".

Bundan əlavə arzuolunmaz nəticələrə əməkdaşların iş fəaliyyətində poçt resurslarından səmərəsiz istifadə olunma da gətirib çıxara bilər. Bunun da əsas səbəbi şirkətdə elektron poçt sisteminin istifadə olunmasına reqlament qoyan qaydaların olmamasıdır. Poçt servisinin səmərəsiz istifadə olunması şirkətin əmək məhsuldarlığının aşağı düşməsinə, əlavə maliyyə xərclərinin sərfiyyatına səbəb olur.

Bir qayda olaraq böyük həcmə malik olan qrafiki, video və səs fayllarının elektron məktublar vasitəsi ilə verilişi şəbəkənin həddən artıq yüklənməsinə və uyğun olaraq əlavə maliyyə xərclərinin yaranmasına gətirib çıxarır. Tədqiqatlar göstərir ki, orta statistik şirkətin poçt resurslarının 30%-i gündəlik olaraq qrafiki, video və səs fayllarının göndərilməsinə sərf olunur. Belə hallarla qarşılaşmamaq üçün, yəni şirkətin vəsaitlərinə nəzərə çarpacaq dərəcədə qənaət etmək üçün məktubların çatdırılmasının yubadılmasından istifadə etmək olar ki, bu da şəbəkənin o qədər də yüklənmədiyi vaxtlarda (məsələn, gecə saatlarında, istirahət günlərində və s.) böyük həcmli informasiyaların verilməsinə imkan verir.

Elektron poçtun xüsusiyyətləri ilə bağlı olan digər bir problem ondan ibarətdir ki, arxivlərdə nəzarət olunmayan və praktiki olaraq silinməsi mümkün olmayan informasiyalar toplanır. Məlumatların ehtiyyat surətləri göndərici və alıcıların personal kompyüterlərində və ya onların işlədikləri şəbəkədə qala bilər. Əgər elektron poçt məlumatları kommersiya xidmətləri və ya internet üzərindən göndərilirsə, o zaman bu proses bir neçə serverdən keçməklə həyata keçiriləcək. Göndərici və alıcı arasında yaradılan "zəncirə" qoşulmuş hər bir server məlumatların surətlərini öz arxivlərində saxlaya bilərlər. Hətta məlumatsurətlərinin silinməsi zamanı elə bir təminat yoxdur ki, bu məlumatlar hər hansı bir kompyüterin diskində və yz serverdə saxlanılmamış olsun. Hamı üçün əlçatan olan proqram təminatının köməyi ilə, hətta sıravi istifadəçi də silinmiş elektron poçt məlumatının yenidən bərpa olunmasını həyata keçirə bilər.



Şəkil 2. İnternet üzərindən elektron poçt məlumatlarının göndərilməsi zamanı yaranan problemlər.

Bütün bu xüsusiyyətlər, həmçinin elektron məlumatın nüsxəsinin çıxarılmasının sadəliyi və bu əməliyyata nəzarət olunmaması, ona gətirib çıxarır ki, əməkdaş anonim olaraq və heç bir icazə olmadan istənilən qədər korporativ informasiyanı həm daxildə yaya bilər, həm də şirkətdən kənara çıxara bilər. Bu zaman bu informasiyalar özündə şirkətin xidməti informasiyalarını (müqavilələrin mətni, planlaşdırılan işlər haqqında məlumat və s.), parolları, sistem verilənləri, proqramların ilkin kodlarını və digər məxfi informasiyaları əks etdirə bilər. Bu isə nəticə etibarı ilə məxfiliyin ciddi surətdə pozulmasına və şirkət üçün arzuolunmaz fəsadların yaranmasına səbəb olar.

Kağızlı əməkdaşlıqdan fərqli olaraq, elektron poçtu asanlıqla və bilərəkdən düzgün olmayan ünvana göndərmək mümkündür. Bunun səbəbi ünvan kitablarından istifadə etmə bacarığının olmaması, alıcının ünvanının səhv göstərilməsi və ya informasiyanın məxfi olması halında təsadüfi olaraq bu informasiyanın böyük bir qrup istifadəçilərə göndərilməsi ola bilər.

Şəbəkədən məxfi informasiyaların sızmasının mühafizəsini təmin etmək üçün alıcılara nəzarət, ötürülən verilənlərin süzgəclənməsi həyata keçirmək və müxtəlif kateqoriyalı istifadəçilərin elektron poçt arxivlərinə girişini məhdudlaşdırmaq lazımdır.

Elektron poçtun əsas fərqli cəhəti ona formal yanaşmanın olmasıdır (digər kommersiyalı kommunikasiyalarla müqayisədə). İlk növbədə əksər istifadəçilər elektron poçta müvəqqəti bir vasitə kimi baxırlar, yəni elektron poçta "oxudum və atdım" prinsipi ilə yanaşırlar. Bu cür yanaşma zamanı mühüm əhəmiyyət kəsb edən informasiyanın silinmə riski mövcuddur. Bundan əlavə ciddi bir müştəri ilə yazışmaların itirilməsi də ola bilər. Bütün bu problemlər təşkilatda elektron poçt arxivinin yaradılması ilə həll edilir.

Şirkətin və onun əməkdaşlarının cinayət məsuliyyətinə cəlb olunması ilə bağlı olan bir sahə-müəllif hüquqlarının pozulmasıdır. Bu hüquqlarla müdafiə olunan materiallar ya elektron poçt məlumatlarında, ya da qoşma fayllarda saxlanıla bilər. Bu materiallara qrafiki, audio, video və müxtəlif növ mətn informasiyaları, yəni elektron formada təsvir edilə bilən və kompyüter şəbəkələri ilə ötürülən istənilən informasiyaları aid etmək olar. Müəlliflərin və ya müəllif hüququ olan şəxslərin icazəsi olmadan bu materialların surətlərinin çıxarılması və yayılması qanun pozuntusu hesab olunur. Əgər şirkət müəllif hüquqları ilə qorunuan poçt materiallarından buna səlahiyyəti olmayan əməkdaşların istifadə etməsi üçün şərait yaradırsa, o zaman şirkət müəllif hüquqlarını pozulmasına görə cinayət məsuliyyətinə cəlb edilə bilər.

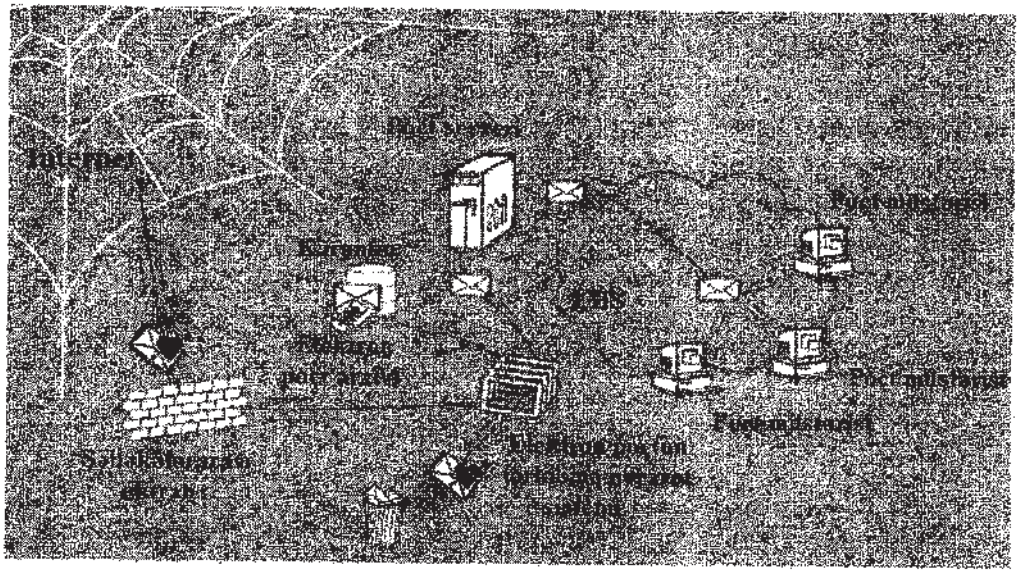
Elektron poçtun istifadə olunası ilə yaranan risklərdən mühafizə olunmaq üçün təşkilatlar uyğun tədbirlər həyata keçirməlidirlər. Mühafizəyə kompleks yanaşma-təşkilati tədbirlərin uyğun texniki vəsaitlərin istifadəsi ilə yaradılması olmalıdır. Təşkilati tədbirlərə şirkətdə elektron poçtun istifadə olunma siyasətinin yaradılması və tətbiqi aiddir. Texniki vəsaitlər bu siyasətin yerinə yetirilməsini həm poçt trafikinin monitorinqi hesabına, həm

də qanun pozuntularına adekvat reaksiyalar hesabına təmin etməlidir.

Qeyd etmək vacibdir ki, elektron poçtun istifadə olunması siyasəti onun reallaşdırılması vasitələri ilə müqayisədə öndədir, çünki, bu siyasət informasiya sisteminin yuxarıda sadalanan risklərdən mühafizəsi üzrə kompleks tədbirlərin yaradılması üçün əsasdır. Əvvəl siyasət formalaşdırmaq, yəni elektron poçtdan istifadə qaydalarını tərtib etmək lazımdır, yaradılmış sistem bu siyasətin müəyyən pozuntularına reaksiya verməlidir, yalnız bundan sonra bu qaydalar elektron poçtun istifadə olunması siyasətinə nəzarət üçün istifadə olunan kompyüter dilinə çevrilməlidir.

Elektron poçtun istifadəsi ilə bağlı yaranan risklərdən şirkətin mühafizə olunması üçün lazımdır:

Elektron poçtun istifadə olunma siyasəti + **Siyasətin reallaşdırılması vasitələri**



Şəkil 3. Poçt sisteminin mühafizə probleminin həlli.

Bu cür texniki vəsaitlərə elektron poçtun tərkibinə nəzarət sistemi (content security software) adlanan xüsusi proqram təminatı aiddir. Bu sistemin funksiyalarına poçt trafikinə nəzarət və elektron poçt üzrə yazışmaların arxivə yerləşdirilməsi daxildir. Yaradılmış sistemə aşağədakı tələblər qoyulur:

- mətn təhlilinin aparılması;
- ötürülən verilənlərin süzgəclənməsi:
  - verilənlərin həcminə və ölçüsünə görə;
  - elektron poçt məlumatlarına edilən əlavələrə görə;
  - faylların növünə görə;
  - elektron poçtun ünvanına görə;
- poçt resurslarının istifadəsinə nəzarət və müxtəlif kateqoriyalı istifadəçilərin bu resurslara girişinin məhdudlaşdırılması;
- cədvəl üzrə təxirə salınan elektron poçt məlumatlarının çatdırılması;
- tam funksiyalı elektron poçt arxivinə giriş.

Bu tələblərin yerinə yetirilməsi mühafizə vasitələrində müəyyən müxanizmlərin tətbiqi ilə təmin edilir. Bu mexanizmlərə aşağıdakılar aiddir:

- rekursiv dekompazisiya (elektron poçt məlumatlarının kompanentlərə ayrılması və onların tərkibinin sonrakı təhlilinin aparılması üçün tətbiq edilən xüsusi alqoritm);
- mətn kodlarının evristik təyin olunması;
- fayl növünün siqnaturaya görə (ikinci və ya üçüncü mənaya görə) təyin edilməsi;
- elektron poçt arxivi üzrə tammətnli axtarış.

Mühafizə vasitəsi-elektron poçtun tərkibinə nəzarət sistemi özlüyündə təhlükəsizliyin təmin olunması ilə bağlı heç bir iş görmür. O, sadəcə yaranmış problemin həllində insana kömək edən "maşındır". Ona görə də bu "maşın" qarşısında təhlükəsizliyin təmin olunması məsələsini qoymaq lazımdır. Bu o deməkdir ki, xüsusi qaydalar hazrlamaq lazımdır ki, gələcəkdə bu qaydalar maşın dilinə çevrilsin. Bu qaydalar yığımı "elektron poçtdan istifadə siyasəti" adlanır.

Bir çox təşkilatlarda uzun illərdir ki, bu qaydalar yığımı artıq mövcuddur. Bəzi məhdudiyyətlər kimi onlar sistemin istifadəçilərinə müəyyən narahatlıqlar yaradır. Bu narahatlıqlardan sonra istifadəçi ya istifadədən imtina edir, ya da qoyulan qadağaları ötüb keçməyə çalışır. Ona görə də yerinə yetirilməsinə nəzarət üçün texniki vəsaitlərdən istifadə olunmayan bu cür siyasət tədricən öz qüvvəsini itirir.

Deməli elektron poçtun istifadə olunma siyasəti elektron poçtun istifadəsi ilə bağlı porsesləri və onların fəaliyyətini reqlamentləşdirən və əməkdaşların təlimatlandırılmasına xidmət edən yazılı şəkildə olan sənədlər toplusudur. Bu sənədlər və təlimatlar hüquqi statusa malikdir və bir qayda olaraq müəssisə əməkdaşlarının təlimatlandırılması üçün təqdim olunur.

Elektron poçtun istifadə olunma siyasəti ümumi korparativ informasiya təhlükəsizliyi siyasətinin vacib elementlərindən biridir. Bu siyasət aşağıdakı kriteriyalara uyğun olmalıdır:

• lokanik və bütün əməkdaşlar tərəfindən başa düşülən olmalı, yazılışın sadəliyi sənədi hüquqi statusunun itirilməsinə gətirib çıxarmamalıdır;

• şirkətin iqtisadi fəaliyyəti prosesində informasiya mühafizəsinin zəruriliyi ön plana çəkilməlidir;

• şirkət daxilində həyata keçirilən digər siyasətlərlə (maliyyə, iqtisadi, hüquqi və s. fəaliyyət sferaları ilə) razılaşdırılmalıdır.

• bir sənəd kimi qanuni qüvvəyə malik olmalıdır, yəni, müəsissənin idarə heyətinin bütün üzvləri tərəfindən imzalanmalı və yerinə yetirilməsi bütün detallarına qədər düşünülməlidir;

• ölkənin ali qanunvericiliyinə zidd olmamalıdır;

• bu siyasətin tələblərini pozan əməkdaşlar haqqında tədbirlər nəzərə alınmalıdır;

• informasiya mühafizəsi dərəcəsi ilə şirkətin əmək məhsuldarlığı arasındakı balans saxlanılmalıdır;

• şirkətin elektron poçtun istifadə olunması siyasətinin təmin olunması üzrə tədbirlər təyin olunmalıdır.

Bir qayda kimi, elektron poçtun istifadə olunması siyasətinə iki cür yanaşma mövcuddur: hüquqi təsdiq olunmuş sənəd kimi və siyasətin reallaşdırılması texnikasını şərh edən material kimi.

Sənəd kimi nələri əks etdirməlidir:

1. Elektron poçtun şirkətin mülkiyyəti olduğunu və yalnız işgüzar məqsədlər üçün istifadə olunmalı olduğunu göstərməlidir.

2. Korparativ elektron poçt sisteminin tətbiqi ali qanunvericiliyə və təhlükəsizlik siyasətinə zidd olmamalıdır.

3. Elektron poçtun istifadəsi və saxlanması üzrə tövsiyyəv və təlimatlar.

4. Şəxsi məqsədlər üçün elektron poçtun sui-istifadə olunması, məhkəmə və xidməti araşdırmalar zamanı əməkdaşların potensial məsuliyyət daşımaları haqqında xəbərdarlıq.

5. Əməkdaşların elektron poçtun istifadə olunması siyasəti ilə tanışlığı haqqında yazılı təminat.

Texniki nöqteyi-nəzərdən bu siyasət elektron poçtdan istifadə qaydalarını, daha doğrusu aşağıdakıları təyin edir:

Nəyə nəzarət olunur	Giriş, çıxış və daxili elektron poçt məlumatlarının hansına icazə verilməli və ya qadağan olunmalı.
Kimlərə paylanılır	Giriş və çıxış elektron poçt məlumatlarının ötürülməsi və alınması icazə verilən və ya qadağan edilən şəxslər.
Sistem necə reaksiya verir	Elektron poçtun istifadə qaydaları ilə təyin edilən kriteriyalara cavab verən və ya cavab verməyən bu və ya digər elektron poçt məlumatları ilə nə etməli?

Elektron poçtdan istifadə siyasətinin yerinə yetirilməsi üçün xüsusi vasitələr tələb olunur. Belə vasitələrə elektron poçtun tərkibinə nəzarət sistemi aid edilə bilər.

Elektron poçtun tərkibinə nəzarət sistemi, elektron poçtun istifadə olunma siyasətinin reallaşdırılması məqsədi ilə müxtəlif kompanentlərə və struktura görə məktubun tərkibini təhlil etmək qabiliyyətinə malik olan proqram təminatıdır.

Bu sistemin əsas xüsusiyyətlərinə aşağıdakılar aiddir:

1. Tərkibin təhlili zamanı xüsusi hazırlanmış elektron məktublardan istifadə olunma siyasətinin tətbiqi.
2. Elektron məktubların "rekursiv dekompazisiyasının" reallaşdırılması imkanı.
3. Müxtəlif maskalanma üsullarından asılı olmayaraq faylların real formatlarının tanınma imkanı.
4. Elektron poçt məlumatlarının parametrlər çoxluğunun təhlili.
5. Elektron poçt arxivinə giriş.
6. Tərkibində qadağan olunmuş sözlərin və ifadələrin olub-olmamasını yoxlamaq üçün elektron poçt məlumatlarının və qoşmaların tərkibinin təhlili.

Elektron poçtun tərkibinə nəzarət sisteminin bütün kateqoriyalarının imkanları spektri kifayət qədər genişdir və istehsalçılardan asılı olaraq bu spektr nəzərə çarpacaq dərəcədə dəyişir. Lakin bütün sistemlərə ümumi tələblər qoyulur ki, onlar da poçt trafikinə nəzarətlə bağlı bütün məsələləri həll etməyə imkan verir.

Belə sistemlərə qoyulan ilk tələblərə bütövlük və adekvatlıq aid edilir.

Bütövlük-nəzarət sisteminin elektron poçt məlumatlarının daha dərindən yoxlanılması qabiliyyətidir. Bu o deməkdir ki, məktubun bütün kompanentləri süzgəcdən keçirilməlidir. Bu zaman elektron məlumatın strukturuna daxil olan heç bir obyekt "diqqətdən kənarda" qalmamalıdır. Məktubların yoxlanılması şərti bütün problemləri, riskləri və təhlükələri nəzərə almalıdır.

Adekvatlıq-bütün qaydaların reallaşdırılması üçün lazım olan vasitələrə malik olmaqdır.

Digər ümumi tələblərə aşağıdakılar aid edilir:

Elektron poçtun mətn təhlili. Bu təhlil məxfi informasiyaların sızmasını aşkar etməyə və vaxtında qarşısını almağa imkan verir.

Elektron poçt məlumatlarının göndərici və alıcılarına nəzarət. Bu nəzarət poçt trafikinin süzgəclənməsinə və bununla da şəbəkələrarası ekranların bəzi funksiyalarının reallaşdırılmasına imkan verir.

Elektron məktubların onları təşkil edən kompanentlərə ayrılması. MIME başlıqlar, məktubun özü, qoşma fayllar və s.

Böyük ölçülü məlumatların gecikdirilməsi və ya blakirovkası. Bu, rabitə kanalının daha az yüklənməsi anına qədər davam edir. Böyük həcmli informasiyaların şəbəkədə sirkulyasiyası şəbəkənin həddən artıq yüklənməsinə səbəb olur. Blakirovka və ya verilişin dayandırılması bunun qarşısını alır.

Qrafiki, video və səs fayllarının tanınması. Bir qayda olaraq bu cür fayllar böyük ölçüyə malik olur və onların şəbəkədə sirkulyasiyası şəbəkə resurslarının məhsuldarlı-

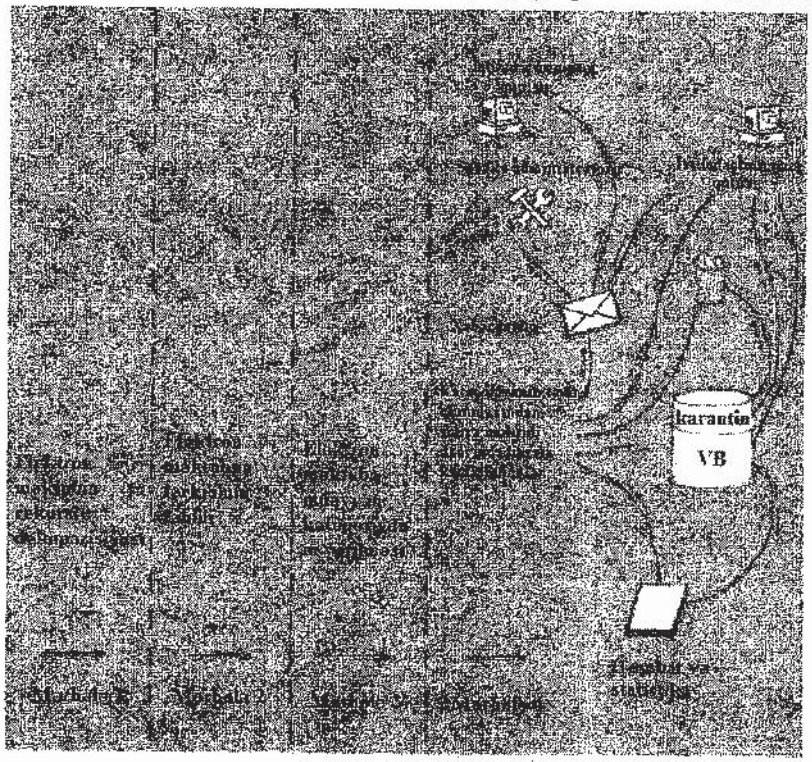
ğının itkisinə gətirib çıxarır. Ona görə də bu növ faylların tanınması və gecikdirilməsi iş effektivliyinin azalmasının qarşısını alır.

Sıxılmış/arxiv faylların emalı. Bu, sıxılmış fayyların tərkibində qadağan olunmuş materialların olub-olmamasını yoxlamağa imkan verir.

Yerinə yetirilən faylların tanınması. Bir qayda olaraq bu cür fayllar böyük ölçüyə malik olur və nadir hallarda şirkətin kommersiya fəaliyyəti ilə əlaqəli olurlar. Bundan əlavə bu fayllar elektron poçt vasitəsi ilə göndərilən əsas virus mənbələridir. Ona görə də bu növ faylların tanınması və verilişinin gecikdirilməsi şirkətin iş effektivliyinin azalmasının qarşısının alınmasına imkan verir.

Tamfunksiyalı elektron poçt arxivinə giriş. Bu arxiv on-line rejimdə böyük həcmli elektron poçt məlumatlarının saxlanılmasını təmin etməlidir. Arxivdə saxlanılan informasiyalar əsasında şirkətin poçt axınının sonrakı təhlilini də həyata keçirmək, sistemin işini korreksiya etmək, münaqişələrin təhlilini aparmaq mümkündür.

Aşağıdakı şəkildə elektron poçtun tərkibinə nəzarət sisteminin işi təsvir olunmuşdur. Məlumatın emalı sxemi bir qayda olaraq, özündə aşağıdakı mərhələləri əks etdirir: elektron məktubun rekrusiv dekompazisiyası; elektron məktubun tərkibinin təhlili; elektron məktubların kateqoriyalara ayrılması; mənimsədilən kateqoriyaya görə məktub üzərində iş.



Şəkil 4. Elektron poçtun tərkibinə nəzarət sistemində məlumatın emalı sxemi.

Xülasə

Məqalə, elektron poçtun istifadə olunması ilə bağlı müəsissə və təşkilatlarda yarana biləcək risklərə, onların yaranma səbəblərinə və bu risklərin və təhlükələrin aradan qaldırılması üsullarına həsr olunmuşdur. Müəsissə və təşkilatlarda əməkdaşların bilərəkdən və ya bilməyərəkdən etdikləri hərəkətlər nəticəsində elektron poçt məlumatlarının korlanması, oğurlanması, məktubların mətnlərininin dəyişdirilməsi və s. bu kimi problemlər işıqlandırılmışdır. Elektron poçt məlumatlarının mühafizəsi və təhlükəsizliyinin təmin olunması üsullarına baxılmış, elektron məktubların tərkininə nəzarət sisteminin yaradılması və təhlükəsizlik tədbirlərinin təsnifatı göstərilmişdir.

Ədəbiyyat:

1. Проскурин В.Г. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. –М.: Радио и связь, 2000.
2. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных /П.Ю.Белкин, О.О.Михальский, А.С. Першаков и др.- М.: Радио и связь, 1999.
3. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları, Dərslik, Bakı, 2009
4. Зегжда П.Д. и др. Теория и практика обеспечения информационной безопасности. – М. Яхтсмен, 1996.
5. Безруков Н.Н. Компьютерные вирусы. - М.: Наука, 1991.
6. Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК. -№8. - 1993.