

7.2 ADQUISICIÓN DE UN FIREWALL
7.2. FIREWALL BAT EROSTEA



¿POR QUÉ Y CÓMO PROTEGER LOS ORDENADORES DE ATAQUES A TRAVÉS DE INTERNET?

ZERGATIK ETA NOLA BABESTU ORDENAGAILUAK INTERNET BIDEZKO ERASOETATIK?

En la actualidad, la cantidad de ordenadores conectados a Internet es elevada, y su número sigue incrementándose paulatinamente. No obstante, al mismo tiempo, aumentan en similar medida los peligros derivados de infecciones por virus informáticos y ataques/intromisiones desde equipos externos.

En este último caso, no sólo se ve comprometida la integridad del sistema o la conexión de red, sino también la información particular de la persona usuaria (o de la red corporativa) ahí almacenada.

Por tal motivo, surge la necesidad de implementar una barrera de seguridad que proteja eficazmente al sistema; aislandolo en gran medida de dicho "entorno peligroso".

«Internet está en una etapa de expansión, cada vez es más común que los ordenadores tengan acceso a este medio y, con ello, a un entorno en el que la transferencia de datos y la conexión entre equipos alcanza un nivel significativo. Así, se plantea un escenario en el que mostrar vulnerabilidades en los equipos o que éstos no estén preparados para soportar intromisiones o ataques externos, supone un riesgo difícilmente aceptable por los sistemas informáticos particulares y empresariales -sobre todo-»

Itziar Goiri, directora de "Gernika MEDIA" (ver ficha anterior: 7.1.), escuchaba atenta a la técnica informática encargada del mantenimiento de la red de ordenadores de su empresa. La verdad, es que ésta le había demostrado la conveniencia de reforzar las medidas de seguridad; si bien es cierto, la desastrosa experiencia sufrida por efecto de un virus (perdió gran parte del trabajo almacenado en sus equipos), colaboró definitivamente en su consideración sobre el "problema".

Gaur egun, ordenagailu asko eta asko daude Interneti lotuta, eta kopuru hori gora doa, poliki-poliki. Dena dela, aldi berean eta antzeko proportzioan ugaritzen ari dira birus informatikoe-ek eragindako arriskuak eta kanpoko ekipoen erasoek/jesku-sartzeek eragindakoak.

Azken kasu horretan, arriskuan daude ez bakarrik sistemaren osotasuna edo sare konexioa, baita sisteman gordetako erabiltzailearen (edo korporazioko sarearen) informazio partikularra.

Hori dela eta, sistema eraginkortasunez babesteko, segurtasun-hesi bat inplementatu behar da; era horretara, "inguru arrisku-tsu" horretatik isolatzen da, maila handi batean bederen.

«Internet zabalkuntza aldian dago orain, gero eta ordenagailu gehiagok dute eremu horretara sartzeko aukera; alegia, datuen transferentziari eta ekipoen arteko loturari dagokionez, goreneko maila iritsi duen eremura sartzeko aukera dute. Hori horrela izanik, partikularren zein enpresen -bereziki- sistema informatikoe-ekin ezin gordeko dute beren burua arriskutik, baldin eta ekipoek ahultasunen bat badute edo ez badaude kanpoko eraso-erregitako prestatuta.»

Itziar Goirik, "Gernika MEDIA" enpresako zuzendariak (ikus aurreko fitxa: 7.1.), adi-adi entzuten zion bere enpresako ordenagailu sareko mantentze-lanak zuzentzen dituen informatikako langile teknikariari. Hark segurtasun-neurriak indartu behar zirela erakutsi zion bere azalpenen bitartez; baina, azalpen haiez gainera, birusaren ondoriozko esperientzia zoritxar hark bultzatu zuten zuzendaria "arazo" hari behin betiko irtenbidea biltzeko erabakia hartzera.

Asimismo, sus percances por infección de virus no habían terminado en el capítulo de "destrucción" anterior; sino que al poco tiempo de este suceso, descubrió que sus PC's de forma autónoma habían enviado a sus contactos (clientela y empresas proveedoras) registrados en su agenda virtual, correos electrónicos infectados por virus (lo supo tras varias llamadas telefónicas de aviso por parte de éstos, ya que las relaciones eran estrechas). Además, tales direcciones también debían de haber sido "capturadas" o robadas de sus equipos, ya que a partir de entonces, casualmente, tales destinatarios eran objetivo de campañas de marketing de carácter "adulto" (... la directora veía como la imagen de la empresa iba perdiendo enteros ...).

Como le señalaba Inés, la técnica informática: *«ltziar, habéis sido víctimas de una infección doble: el primero de los virus se ha intentado propagar a través de vuestra agenda electrónica y también ha transmitido información confidencial -como los correos- a determinado destino fraudulento; mientras que el segundo, ha tenido un efecto más letal, y ha destruido archivos esenciales almacenados en los ordenadores, empleando la red local como vía de transmisión».*

Por tales motivos -insistía-, además de la instalación de un antivirus, era necesario aislar los ordenadores pertenecientes a la red local de Internet y, esta función de control y "vigilancia", la realizan los firewall o cortafuegos. La técnica informática vuelve a su labor docente (es la directora quien la reclama; y quien paga por horas...) y explica que se trata de dispositivos o programas informáticos que inspeccionan las transmisiones y conexiones (de entrada y salida) que realizan los ordenadores; permitiendo (o bloqueando) su paso en función de los criterios de seguridad con los que hayan sido configurados (el firewall actúa como un filtro). Obviamente, una de sus misiones más relevantes es proteger la información de ataques generalmente cometidos por personas no autorizadas (ataques externos e incluso internos -de la misma red local-).

La técnica informática admitía que, ciertamente, no era un elemento de seguridad popular: *«frente al amplio conocimiento -y empleo- que existe sobre los antivirus y su relevancia, el papel de los firewall no es tan conocido -en general- entre el conjunto de personas usuarias informáticos. Sin embargo, su función como barrera de defensa en los equipos es esencial; sobre todo, en aquellas empresas -como la vuestra- que cuentan con un sistema informático (conjunto y/o red de ordenadores) que se encuentra conectado a Internet de forma permanente (ADSL, Cable,...); ya que resulta más "sencillo" a las personas intrusas encontrar una puerta abierta a la información confidencial almacenada en los equipos».*

Y, como la infección sufrida por "Gernika MEDIA" resultaba un buen ejemplo, la informática apuntó que el firewall también controla la información que "sale" del ordenador. Esta función es fundamental, ya que existen numerosos virus o programas espía que, una vez se han infiltrado en los equipos, transmiten información sobre el sistema y comunican datos (a través de Internet) a terceras personas; todo ello sin requerir ningún consentimiento previo.

Como ltziar aún no comprendía bien el funcionamiento de los cortafuegos, ella prosiguió: *«los firewall -básicamente- rechazan cualquier tipo de tráfico no autorizado entre el equipo y la red en la que se encuentre (Internet o corporativa). Esto quiere decir que, a medida que se necesite otorgar permisos a distin-*

Bestalde, birusaren ondoriozko ezbeharrak ez ziren aurreko ataleko "suntsiketa" horretan gelditu; hura gertatu eta denbora gutxira ohartu ziren PCek birus batez kutsatutako posta elektronikoa bidali zizkietela, era autonomoan, agenda birtualean erregistratuta zituzten kontaktu guztiei (bezeroak eta enpresa hornitzaileak); haiek telefonoz eman zieten haren berri, enpresaren eta bezeroen arteko harremanak oso estuak baitziren. Bestalde, helbide haiek beren ekipoetatik "hartu" edo lapurtu egin bide zituzten, eta ordutik aurrera, hartzaile haiek, ustekabean, "nagusiei" zuzendutako marketing kanpainen helburu bihurtu ziren (... zuzendaria ohartzen ari zen bere enpresaren irudiarentzat kalte handiak zirela haiek...).

Inesek, informatikako langile teknikariak, honela esan zion zuzendariari: *«ltziar, infekzio bikoitza jasan duzue: lehenengo birusa agenda elektronikoaren bitartez zabaltzen saiatu da, eta isilpeko informazioa bidali du -postak, esaterako-, iruzurrezko helbideetara; bigarren birusak, aldiz, eragin latzagoa izan du, eta ordenagailuetan gordeta zeuden oinarriko artxiboak deuseztatu ditu, eta bertako sarea erabili du transmisiorako».*

Horren guztien ondorioz -zioen behin eta berriro langile teknikariak-, antibirus bat instalatzeaz gainera, sare lokaleko ordenagailuak Internetetik bakandu behar ziren; kontrol eta "zainketa" funtzio hori firewall edo suebakiak betetzen dute. Informatikariak irakasle papera hartu du berriro ere (zuzendariak eskatu dio horrela egiteko; orduka ordaintzen dio...), eta azaltzen du tresna berri horien zeregina: ordenagailuen transmisioak eta konexioak (sarrera eta irteera) ikuskatzen dituzten tresna edo programa informatikoak dira; transmisio horiei baimena ematea (edo blokeatzea) konfigurazioan kontuan hartu diren segurtasun-irizpideen arabera da (firewall edo suebakiak irazkiaren zeregina betetzen du). Jakina, tresna horien zeregin nagusietako bat da baimena ez duten pertsonen erasoetatik (kanpoko erasoak zein barrukoak -sare lokalekoak-) informazioa babestea.

Informatikako langile teknikariak onartzen zuen suebakia ez zela segurtasun osagai ezaguna *«antivirusak oso ezagunak dira -oso erabiliak- eta garrantzi handikoak, baina firewall osagaien zeregina ez da hain ezaguna -oro har- erabiltzaile informatikoen artean. Dena dela, babeserako hesi gisa betetzen duen funtzioa oinarrikoa da ekipoentzat; batez ere, Internetera etenik gabe lotuta dagoen (ADSL, Kablea...) sistema informatikoa duten (ordenagailu multzoa eta/edo sarea) enpresetan -zurea adibidez-; era horretako sistemetan kanpotarrentzat "errazagoa" baita ekipoetan gordeta dagoen isilpeko informazioa sartzeko ate bat zabalik aurkitzea».*

Eta "Gernika MEDIA" enpresan gertatutako infekzioa oso adibide ona zenez, informatikako langile teknikariak adierazi zuen firewall osagaiak kontrolatuko ziela zer informazio "irteten" den ordenagailutik. Funtzio hori ezinbestekoa da, birus edo programa espioi ugari baitaude ekipoetan sartu eta sistemari buruzko informazioa beste pertsona batzuei transmititzen eta datuak jakinarazten dizkietenak (internet bidez); eta hori guztia aurretik baimenik lortu gabe egin dezakete.

ltziarrek suebakiaren funtzionamendua ondo ulertu ez zuenez, aurrera jarraitu zuen langile teknikaria bere azalpenekin: *«firewall edo suebakiak -oinarrian- baztertu egiten dute ekipoaren eta sarearen artean (Internet edo sare lokala) baimenik gabeko garraioa. Horrek honakoa adierazi nahi du: Internetera sarbidea eduki behar duten aplikazioei baimena eman ahal, firewalla konfiguratzeko joango da, aipatutako beharrei erantzute-*



tas aplicaciones que deban tener acceso a Internet, se irá configurando adecuadamente el firewall para dar respuesta a las necesidades presentadas. De esta manera, la transmisión/recepción de datos quedará fijada en todo momento por el consentimiento declarado al cortafuegos por la persona usuaria del equipo o red. Además, si por cualquier razón se intentara establecer una conexión o acceso no autorizado -como hizo el virus-, el firewall mostrará un mensaje de alerta, señalando el servicio o programa que está intentando acceder a la red de "dentro a fuera" o a la inversa; posibilitando una adecuación o nueva configuración si así fuera necesario».

Itziar ya lo tenía todo claro, y era capaz de entender que dos de los principales beneficios de la implementación de un firewall serían:

- La seguridad de los equipos.
- La integridad de la información en ellos contenida.

Así, y como justificación final de lo expuesto, la informática señaló que esta importante tarea desarrollada por el firewall, debería estar complementada por un antivirus correctamente actualizado (aquél que ya habían acordado instalar). Recordando que el cortafuegos permite o restringe el tráfico de datos, pero no comprueba el carácter o contenido de los mismos; labor que sí efectúa el antivirus y que explica la importancia de contar con ambos "elementos" trabajando conjuntamente.

ko. Era horretara, datuak transmititzea/hartzea ekipoaren edo sarearen erabiltzaileak suebakiari aitortutako onepenaren araberakoa izango da, beti. Eta edozein arrazoiengatik baime-nik gabe sartzeko edo konektatzeko saiorik egongo balitz -birusak egin zuen bezala-, firewallak erne egoteko mezua erakutsiko du, eta bertan agertuko da zer zerbitzu edo programa ari den "kanpotik barrura" sartzeko saioa egiten, edo alde-erantziz; horrek aukera ematen du egoera horretara egokitzeko edo konfigurazio berri bat osatzeko, hala behar izanez gero».

Itziarrek argi ikusten zuen, eta azalpen horien bitartez, ohartzen zen firewall bat inplementatzeak bi abantaila hauek ekarriko lizkiokela:

- Ekipoen segurtasuna.
- Ekipoetako informazioaren osotasuna.

Azaldutako guztiaren azken justifikazio gisa, informatikako langile teknikariak adierazi zuen firewalllek egindako garrantzizko lan hori, behar bezala eguneratutako antibirus batekin osatu beharko litzatekeela (aurretik jartzea erabaki zuten hura). Bestalde, gogorarazi zien suebakiak datuen garraioa onartzen edo mugatzen duela, baina ez duela horien izaera edo edukia egiaztatzen; lan hori, ordea, antibirusak egiten du, eta horregatik, garrantzi handikoa da bi "osagai" horiek edukitzea, biak elkarlanean aritu daitezen



En la actualidad, dado el carácter y la utilización del canal Internet como medio de comunicación entre equipos (y personas), resulta fundamental el empleo de un firewall en aquellos ordenadores que tengan acceso a dicha red (como mínimo). De este modo, se garantizará un adecuado nivel de seguridad, y se eliminará o minimizará el riesgo asociado a estar en conexión a la Red: ataques externos, intrusiones, "robo" de información confidencial,...

En concreto, su utilización en el ámbito empresarial debería ser indispensable; atendiendo al carácter de la información o datos tratados en dicho entorno, y a la importancia de la integridad de los equipos de tales sistemas (soportan su actividad).

De igual manera, no debería plantearse únicamente su trabajo aislado, sino en combinación con un programa antivirus que complete la barrera de seguridad:

- El firewall controlaría el tráfico de datos (entrada/salida).
- El antivirus analizaría los datos y desinfectaría (si fuera necesario) aquéllos portadores de virus informáticos.

Gaur egun, ezinbestekoa da firewall bat erabiltzea Internetera sarbidea duten ordenagailuetan (horietan, gutxienez), sare horrek duen izaera eta ekipoen arteko (eta pertsonen arteko) komunikabide gisa duen erabilera dela-eta. Era horretara, segurtasun maila egokia bermatzen da, eta Sarera konektatuta egoteak berarekin dakarren arriskua deuseztatu edo murriztu egiten da: kanpoko erasoak, sarkinkeria, isilpeko informazioa "lapurtzea",...

Zehazki, firewallak ezinbestekoa beharko luke enpresaren eremuan; kontuan hartuta eremu horretan lantzen den informazioaren edo datuen izaera, eta sistema horietako ekipoen osotasuna (haien jarduerari eusten diote).

Bestalde, tresna horren lana ez bakanduta hartu behar, baizik eta antibirus programa batekin batera, segurtasun hesia osatzeko moduan:

- Firewallak datuen joan-etorria kontrolatzen du (sarrera/irteera).
- Antibirusak datuak aztertzen ditu eta (behar izanez gero) birus informatikoarekin kutsatuta daudenak desinfectatzen.