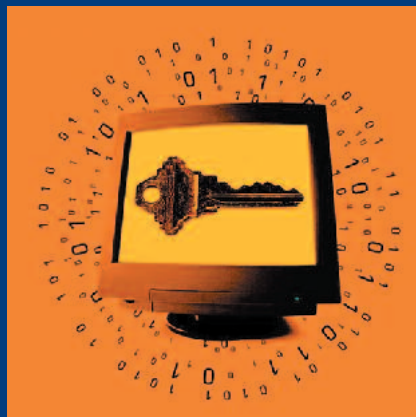


7.1 ADQUISICIÓN DE UN ANTIVIRUS 7.1. ANTIBIRUS BAT EROSTEA.



EL PORQUÉ DE LA COMPRA DE UN ANTIVIRUS ANTIBIRUS BAT EROSTEKO ARRAZOIAK

A medida que aumenta el número de personas usuarias de equipos informáticos, y la conexión a Internet, se incrementa la probabilidad de padecer el ataque de un virus informático. Cada vez es mayor la cantidad de documentos y archivos compartidos, o la cantidad de datos recibidos/transmitidos a través de redes corporativas o Internet; por lo que la capacidad de los virus para extenderse e infectar equipos no para de crecer.

Ante este panorama preocupante e inseguro, resulta necesario adoptar las medidas que garanticen la "salud" e integridad de los ordenadores; de otra forma, se vería comprometida cualquier actividad con soporte informático.

Es común escuchar con cierta frecuencia en los medios de comunicación los perjuicios y problemas que ha causado la infección de determinado virus informático. En especial, resulta sorprendente la traducción económica del impacto de dicho virus, sobre todo cuando se cuantifica su incidencia, los problemas causados y las pérdidas que ha generado en el ámbito empresarial.

Por ello, queda claro que son significativamente perjudiciales, produciendo sus efectos nocivos un detrimento en la actividad de cualquier empresa que emplee equipos informáticos. Pero, ¿qué son los virus?; se conoce su carácter negativo, no obstante, aún persiste una idea vaga sobre su identidad y forma de entrada en los ordenadores. Motivos que explican el frecuente desconocimiento a la hora de obstaculizar las infecciones...

... este "desconocimiento" fue la razón principal por la cual los ordenadores de "Gernika MEDIA", empresa dedicada al des-

Informatika tresnen erabiltzaile kopurua handitu eta Internetarako konexioa ugaltu ahala, handitu egiten da birus informatiko baten eraso jasateko probabilitatea. Gero eta agiri eta artxibo gehiago partekatzen dira, eta gero eta datu gehiago jasotzen eta igortzen dira, korporazioetako sareen edo Interneten bidez; horren guztiaren ondorioz, etengabe ari da zabaltzen birusak ugaltzeko eta ekipoak kutsatzeko ahalmena.

Egoera kezkarri eta ezegonkor horren aurrean, ezinbestekoa da ordenagailuen "osasuna" eta segurtasuna bermatuko duten neurriak hartzea; bestela, arriskuan egongo bailitzateke euskarri informatikoan egindako edozer jardura.

Komunikabideetan, nahiko maiz entzuten da birus informatiko jakin batek eragindako kalte eta arazozen berri. Harrigarria da birus horrek ekonomiaren alorrean izan dezakeen eragina, bereziki, enpresaren alorrean izan duen eragina eta sortu dituen arazoak eta galerak kuantifikatzen direnean.

Beraz, argi dago birusek kalte handiak eragiten dituztela, eta ondorio kaltegarriak dituztela ekipo informatikoak erabiltzen dituen edonolako enpresaren jardueran. Baina, zer da birus bat?; badakigu izaera negatiboa duela, hala ere, birusaren nortasunari eta ordenagailuetan sartzeko moduari buruzko ikuspegia lausoa da gaur egun, oraindik. Hori dela eta, ohikoa izaten da infekzioei oztopoak jartzeko moduari buruzko ezjakintasuna...

... "Ezjakintasuna" izan zen, hain zuzen ere, "Gernika MEDIA" ikus-entzunezko edukiak lantzen diharduen enpresak bere disko gogorretako fitxategiak galtzeko arrazoi nagusia...

arrollo de contenido audiovisual, perdieran todos los ficheros de sus discos duros ...

Esta PYME, dada su actividad, hacía un uso intensivo de los equipos informáticos; representando una herramienta imprescindible, sin la cual, le resultaría imposible realizar cualquiera de los trabajos que ofertaba. Por otro lado, la plantilla de la empresa empleaba frecuentemente el correo electrónico para comunicarse con la clientela, enviándoles bocetos, recogiendo sus pedidos, etc. Por ello, era muy habitual la comunicación a través del canal Internet (ciertamente, representaba una clara ventaja: comodidad y rapidez).

Realmente, Itziar Goiri, directora de "Gernika MEDIA", estaba satisfecha con los potentes equipos de la empresa; además de encontrarse adecuadamente actualizados, todos estaban en red (para compartir archivos y periféricos como la impresora o el escáner entre ellos) y disponían de conexión a Internet. Sin embargo, no contaban con ninguna aplicación que les protegiera de ataques externos (vía Internet) o virus; ya que Itziar nunca había considerado esta necesidad.

Este fue su grave error, "olvidar" (o desconocer) que una fuente principal de propagación e infección de virus es el correo electrónico...

Así, un "buen día", las personas trabajadoras de la empresa comprobaron como una parte significativa de sus archivos ya no existían, y que algunos de sus ordenadores ni siquiera funcionaban. La directora, desconcertada, avisó a Inés, la informática que llevaba el mantenimiento de sus equipos. En los PC's estaba el trabajo de la última semana (del cual no les había dado tiempo a realizar la periódica copia de seguridad); a su vez, tenían que entregar un proyecto para dentro de tres días, y necesitaban los equipos inmediatamente (pensaba alarmada Itziar)...

Una vez se encontró en la empresa, la informática no tardó en descubrir que la causa de la "tragedia" había sido un virus informático que había llegado a través de un correo electrónico y, lo más grave de todo, que no era posible recuperar los archivos perdidos. ¿Solución?:

- "Pasar" un antivirus para eliminarlo totalmente.
- Reinstalar todas las aplicaciones necesarias en parte de los ordenadores.

En cuanto al trabajo perdido y el proyecto presente; el primero debía comenzarse desde el principio, mientras que el segundo tenía que esperar hasta que el sistema informático de "Gernika MEDIA" volviese a la normalidad.

Tras esta fatalidad, la directora decidió, a la vez que proteger adecuadamente su sistema de los virus, conocer qué eran exactamente y cómo protegerse eficazmente contra ellos (se había convertido en una cuestión personal). Encargó a la técnica el "blindaje" de su red de ordenadores y cierta labor docente:

La informática, explicó a la propietaria que los virus son programas (por lo general, de tamaño reducido) que se introducen sin permiso en los ordenadores para producir -generalmente- efectos no deseados y nocivos; y que poseen una característica principal: alteran el funcionamiento de los equipos (una vez se ha introducido en el ordenador) sin ningún

ETE honek, bere jarduera dela-eta, era intentsiboan erabiltzen zituen tresna informatikoak; ezinbesteko tresna ditu ordenagailuak, eta horiek gabe ezin egingo lituzke eskaintzen dituen lanak. Bestalde, enpresako langileek etengabe erabiltzen zuten posta elektronikoa, bezeroekin harremanetan jartzeko, zirriborroak bidaltzeko, eskariak jasotzeko, etab. Hori dela eta, ohikoa zen Internet bidezko komunikazioa (horrek abantaila nabarmena zekarkion enpresari: alegia erosotasuna eta lastertasuna).

Itziar Goiri, "Gernika MEDIA" enpresako zuzendaria, oso gustura zegoen enpresako tresna ahaltzu haiekin; behar bezala eguneratuta egoteaz gainera, guztiak sarean zeuden (artxiobak eta periferikoak partekatu ahal izateko, hala nola, inprimagailua edo eskanerra), eta guztiak zuten Internetera sartzeko aukera. Hala ere, ez zuten kanpoko erasoetatik (Internet bidez) edo birusetatik babesten zituen aplikaziorik; izan ere, Itziarrek ez zuen inoiz horren beharrik ikusi.

Horixe izan zen, hain zuzen ere, egin zuen akats larriena, hau da, birusak zabaltzeko edo infektatzeko bide nagusia posta elektronikoa dela "ahaztu" zuen (edo ez zuten horren berri).

Hala, "egun batean", langileak ohartu ziren artxibo asko desagertuak zirela, eta ordenagailu batzuk ez zebiltzala. Zuzendaria harri eta zur gelditu zen, eta Inesi deitu zion, informatikako tresnen mantentze-lanen arduraduna. PCetan azken asteko lana zegoen (ez zuten aldi behingo segurtasun kopia egiteko denborarik izan); bestalde, hiru egunen buruan proiektu bat amaitu behar zuten, eta ezinbestekoak zituzten ekipoak (zion bere buruari Itziarrek, larri)...

Informatikako langile teknikaria enpresara iritsi eta berehala konturatu zen zein zen "tragedia" haren arrazoa: posta elektronikoa bidez iritsitako birus informatiko bat izan zen eragilea. Baina bazen okerragorik, ezin berreskura zitezkeen galdutako artxiobak. Zer irtenbide zuten, ordea?:

- Antibirus bat "pasarazi", birusa erabat suntsitzeko.
- Zenbait ordenagailutan beharrezko aplikazio guztiak berriro instalatu.

Galdutako lanari zegokionez, hutsetik hasi beharko zuten berriro, eta esku artean zuten proiektuari zegokionez, "Gernika MEDIA"-ko sistema informatikoa normaltasunera iritsi arte itxaron beharko zen, ez zegoen beste irtenbiderik.

Zoritzarreko gertaera haren ondoren, zuzendariak erabaki zuen ondo babestu behar zuela bere sistema birusen aurrean; baina horrez gainera, birusak zehazki zer ziren jakin nahi zuen, eta halaber jakin nahi zuen haien aurrean eraginkortasunez nola babes zitekeen (arazo pertsonal bihurtu zen). Informatikako langileari agindu zion ordenagailu sarea "blindatzea" eta nolabaiteko irakaskuntza lana egitea:

Informatikako langile teknikariak zuzendariari azaldu zion birusak programak izaten direla (tamainaz txikiak, oro har), eta baimenik gabe sartzeko direla ordenagailuetan, ondorio kaltegarriak eragiteko xedearekin. Birusen ezaugarri nagusia honako hau da: ekipoen funtzionamendua kaltetzen dute (behin ordenagailuan sartzeko direnean), erabiltzailearen baimenik edo onespenean jaso behar gabe. Eta kalte txikiagoak eragiten dituzten birus ugari badaude ere, enpresa hark birus suntsitzaileenetako baten eraso jasan zuen (zoritxarra?).



tipo de autorización o consentimiento por parte de la persona usuaria. Y aunque existen multitud de virus con efectos menos nocivos, su empresa había sufrido el ataque de uno de los más destructivos (¿mala suerte?).

Ante la pregunta "¿por dónde acceden?" que formulaba insistentemente Itziar, la informática recalcó que los virus para atacar los ordenadores entran "sin permiso"; por ello, su acceso se trata de un factor clave que hay conocer previamente para minimizar las posibilidades de infección. De este modo, hizo un repaso de las principales vías de entrada:

- **Unidades de disco extraíbles:** disquetes, CD's,... En estos soportes de almacenamiento pueden encontrarse los virus que, una vez se hayan ejecutado o trasladado al equipo, infectarán éste.
- **Internet:** A través de este medio o canal de comunicación, se establece una conexión en la se transfiere información y datos: navegación por páginas Web, descarga de archivos (música, videos, programas,...), envío/recepción de correo electrónico, etc. Por lo tanto, los virus encuentran el escenario idóneo para introducirse e infectar los equipos de aquellas personas usuarias desprotegidas. En concreto, caben destacar los riesgos que encierran los mensajes electrónicos con ficheros adjuntos (esto le interesaba a la directora); en especial, cuando el emisor es desconocido (existen ciertos virus que se auto-reenvían mediante el correo electrónico sin conocimiento del propietario del equipo). Además, también es posible que el ordenador se infecte simplemente visitando páginas Web; ya que éstas pueden alojar determinados programas con virus.

Por todo lo expuesto, y la experiencia sufrida, Itziar comprendió finalmente la necesidad de poner barreras contra los virus y proteger los ordenadores de sus poco deseables efectos, siendo ésta una medida de seguridad ineludible dentro de los sistemas informáticos empresariales. Y, como subrayó el técnico informática, esta función de contención, prevención y "cura" la cumplen los **antivirus**.

Sin mostrar ninguna "molestia", el informática-formadora siguió con su lección. Explicó a Itziar que los antivirus, fundamentalmente, son programas especializados en detectar y eliminar virus de los ordenadores. Básicamente, analizan la memoria y las unidades de disco de los equipos en busca de virus; puesto que los virus informáticos se diferencian entre sí por su código. Los antivirus rastrean los patrones (códigos de virus que "conocen": definiciones de virus) en todos los archivos del ordenador y, una vez han detectado alguno de ellos, informan a la persona usuaria y proceden a desinfectar el fichero.

Lógicamente, este proceso exige la identificación previa de los virus y, por tal motivo, los antivirus cuentan con un extenso listado de virus en el que se localizan aquéllos conocidos y las medidas adecuadas para su eliminación del sistema. Sin embargo, como había señalado anteriormente, la informática insiste en que diariamente surgen nuevos virus, y las empresas desarrolladoras de antivirus elaboran vacunas para los mismos; por ello, es esencial contar con el comentado listado de virus permanentemente actualizado. De otra forma, la utilidad del antivirus quedaría ciertamente mermada. No obstante, es posible acceder a las nuevas vacunas a través de Internet; en la mayoría de las ocasiones, los propios antivirus

"Nondik sartzen dira, ordea?" galdetzen zuen etengabe Itziarrek, eta informatikako langile teknikoak azpimarratu zion birusak "baimenik gabe" sartzen direla ordenagailuetan, haiek erasotzeko helburuarekin; hori dela eta, birusen sarbidea garrantziko faktorea da, eta aurretik jakin behar da, infekzioaren aukerak murrizteko. Beraz, sarbide nagusien erreposoa egin zuen:

- **Disko unitate aldagarriak:** disketeak, CDak,... Birus mota batzuk gauzak biltegitzeko euskarri horietan egoten dira, eta tresna horiek ekipora eraman edo sartzen direnean, ordenagailua kutsatzen dute.
- **Internet:** Baliabide edo komunikazio bide honen bitartez, informazioa eta datuak igortzeko konexioa lortzen da: Web orrialdeetan nabigatu, artxiboak jaitsi (musika, bideoak, programak...), posta elektronikoa bidali/jaso, etab. Beraz, baliabide egokia da birusentzat babestu gabeko erabiltzaileen ekipoetan sartu eta haiek kutsatzeko. Bereziki kontuan hartu behar dira erantsita fitxategiak dituzten mezu elektronikoak (hori oso interesgarria zen zuzendariarentzat), eta, batez ere, igorlea ezezaguna den kasuetan (zenbaitetan, birus batzuek beren buruaren kopia bat bidaltzen dute posta elektronikoaren bitartez, eta ekipoaren nagusiak horren berri jakin gabe). Horrez gainera, gerta liteke ordenagailua Web orri jakin batzuk bisitatu hutsarekin kutsatzea; orri horietan birusa duten hainbat programa egon baitaitezke.

Hori guztia kontuan hartuta, eta izandako esperientziaren ondorioz, Itziar ohartu zen birusen kontrako oztopoak jarri behar zirela, eta ordenagailuak birus haien ondorioetatik babestu behar zirela; segurtasun neurri hori saihestezina da enpresetako sistema informatikoei dagokienez. Eta informatikako langile teknikariak esan bezala, **antibirus**ek betetzen dute birusari eusteko, aurea hartzeko eta "sendatzeko" funtzioa.

Informatikako teknikaria eta prestatzaileak bere ikasgaiarekin jarraitu zuen, inongo "arazorik" gabe. Itziarri azaldu zion birusak ordenagailuetan hautematen eta horiek deuseztatzen espezializatutako programak direla antibirusak, oinarrian. Birusaren bila dabiltzala, ekipoen memoria eta disko unitateak aztertzen dituzte; birus informatikoak beren kodeagatik bereizten baitira batzuk besteetatik. Antibirusen patroiak arakatzen dituzte ("ezagunak" diren birusen kodeak: birusaren definizioak) ordenagailuetako artxibo guztietan, eta birus bat antzematen dutenean, erabiltzaileari horren berri eman eta fitxategia desinfectatzeari ekiten diote.

Prozesu hori abian jar dadin, ezinbestekoa da birusak aurretik identifikatzea; hori dela eta, antibirusen birus zerrenda luze bat dute, eta bertan, birus ezagunak eta horiek sistematik kentzeko neurri egokiak agertzen dira. Dena dela, informatikako teknikariak behin eta berriro adierazi zuen eguneroko sortzen direla birus berriak, eta antibirus enpresak etengabe dihardutela horientzako txertoak bilatzen; horregatik, ezinbestekoa da aipatutako birus zerrenda hori etengabe eguneratzea. Hala gertatuko ez balitz, antibirusaren erabilgarritasuna murriztu egingo litzateke. Eta kontuan hartu behar da Internet bidez ere lor daitezkeela txerto berriak; gehienetan, antibirusak berak eguneratzen dira era automatikoa, eta beren lana ondo egingo dutela bermatzen dute.

Azkenik, birusari lotutako arriskuak azaldu ondoren, eta zuzendariaren eskaerak kontuan hartuta, informatikako techni-

se actualizan automáticamente y garantizan el éxito de su trabajo.

Por último, tras explicar los peligros asociados a los virus, y ante los requerimientos de la directora, la técnica informática pasó a listar una serie de recomendaciones con el objeto de reproducir un entorno seguro:

- Realizar un análisis sobre los riesgos o peligros a los que puede estar expuesto el sistema informático de la empresa.
- Emplear un antivirus correctamente configurado.
- Mantener el antivirus permanentemente actualizado (a través de Internet).
- Programar la realización de copias de seguridad periódicas (Ficha 7.3.).
- Instalar un firewall (**ver siguiente Ficha: 7.2.**)
- Mantener el Sistema Operativo y las aplicaciones actualizadas.
- Promover un comportamiento "seguro"; es decir, que las personas usuarias mantengan una conducta en términos informáticos precavida: no abriendo mensajes de correo de personas desconocidas (sobre todo, si tienen un archivo adjunto), verificando el contenido de disquetes y CD's antes de su ejecución, vigilando la descarga de archivos de Internet, manteniendo activo en todo momento el antivirus, etc.
- ...

Una vez la técnico informática hubo introducido a Itziar Goiri en el apasionante mundo de los virus, sólo quedaba la instalación definitiva de un antivirus en los ordenadores de la empresa; pero... la informática aprovechó la ocasión (le gustaban los trabajos bien hechos) y advirtió a la directora de la necesidad de contar con otro elemento de seguridad fundamental: un firewall o cortafuegos (pero esto ya es otra ficha: 7.2.)

kariak hainbat gomendio eman zizkion enpresan inguru segurua lor zezan:

- Enpresako sistema informatikoak izan ditzakeen arriskuei buruzko analisisa egin.
- Behar bezala konfiguratu den antibirusa erabili.
- Antibirusa etengabe eguneratu (Internet bidez).
- Aldian-aldian segurtasun kopiak egiteko zeregina programatu (7.3. fitxa).
- Firewall bat instalatu (**ikusi fitxa hau: 7.2.**)
- Sistema operatiboa eta aplikazioak eguneratu.
- Jokabide "segurua" sustatu; hau da, erabiltzaileek jarrera zuhurra izan behar dute, informatikari dagokionez: ezezagunek igorritako posta mezuak ez zabaldu (bereziki, artxi- bo bat erantsita dutenean), diskete eta CDen edukia erabili aurretik egiaztatu, Internetetik jaisten diren artxi- boei adi egon, antibirusa denbora guztian aktibatuta eduki, etab.
- ...

Itziar Goiri birusen mundu liluragarria erakutsi ondoren, informatikako langile teknikariak gauza bakarra gelditzen zela aipatu zuen: antibirus bat instalatu behar zen enpresako ordenagailuetan; baina... egoeraz baliatuta, beste segurtasun osagai bat ere egokia zela adierazi zion langile teknikariak (lanak ondo egitea gustatzen zitzaion): firewall edo suebaki bat instalatzea komeni zen (baina honi beste fitxa bat dagokio: 7.2.).

Los programas antivirus, actualmente, se convierten en un requisito imprescindible para los sistemas informáticos empresariales. Es tal el número de virus, su ritmo de crecimiento, el alcance de éstos y el perjuicio que generan en los equipos, que el que estos no estén debidamente protegidos frente a su ataque, representa un riesgo que ninguna empresa puede asumir.

En este sentido, el software antivirus es un elemento (medida de seguridad) que beneficiará a la actividad empresarial:

- Evitará los problemas (económicos, sobre todo) derivados de la pérdida de información o inutilización de los equipos.
- Facilitará la continuidad del trabajo al promover un medio sin interrupciones o alteraciones por virus.
- Protegerá la confidencialidad de la información (existen modalidades de virus que "abren puertas" en las redes corporativas).
- ...

Antivirus programak, gaur egun, ezinbesteko baldintza dira enpresetako sistema informatikoetan. Birus kopurua izugarria da, haziera erritmoa handia dute, helmen handikoak dira, eta kalte handiak eragiten dituzte; beraz, ekipoak ez badira erasoaren aurrean behar bezala babesten, ez dago arrisku horri aurre egingo dion enpresarik.

Zentzu horretan, antibirus softwarea mesede handiko osagaia da (segurtasun neurria) enpresaren jardunari dagokionez:

- Informazioa galtzea edo ekipoak ezin erabili gelditzea saihestuko da (batez ere, arazo ekonomikoak saihesten dira).
- Lanaren jarraipena erraztuko du, birusaren ondoriozko etenik edo aldaketarik gabeko ingurua osatuko baita.
- Informazioaren isilpekotasuna babestuko da (zenbait birusek korporazioetako sareetako "ateak ere zabaltzen").
- ...