SISTEMAS INFORMATICOS

FORO EVALUABLE 2

ALUMNO CESUR 24/25

Alejandro Muñoz de la Sierra

PROFESOR

Efren Zurita Alonso

Protección contra el malware en la empresa

Un tiempo atrás tuvimos un episodio inesperado: un troyano se coló en nuestra red, causando un desorden bastante notable. Sí, logramos restablecer nuestros sistemas a tiempo, pero la experiencia nos recuerda, en la mayoría de los casos que bajar la guardia en ciberseguridad es un lujo que no podemos permitirnos.

Te cuento de manera informal lo que normalmente ocurre y cómo podemos estar mejor preparados. No es raro que distintos tipos de malware se reinventen para colarse sin que nos demos cuenta, por lo que vale la pena repasar las amenazas y las medidas que podemos tomar.

Empecemos por echarle un vistazo a los "invasores":

• Los **virus** se esconden en archivos que parecen inocuos y se activan apenas los abrimos. Pueden viajar por correos, USB infectados o incluso descargas de dudosa procedencia. Seguro recuerdas el infame “ILOVEYOU” del 2000, que se propagó por email y dejó un agujero en el bolsillo a muchas empresas.

• Luego están los **gusanos**, que se replican casi solos, desplazándose por redes y correos sin necesidad de que toquemos nada. Un ejemplo de esto es “WannaCry” (2017), que interrumpió servicios en empresas y hospitales, exigiendo rescates en bitcoins.

• Los **troyanos** son esos programas que aparentan ser legítimos para lograr engañarnos y entrar sin que sospechemos: el famoso “Zeus” se dedicaba a robar credenciales bancarias, pasando desapercibido.

• El **spyware** se instala sin pedir permiso y, poco a poco, recoge información personal —desde contraseñas hasta hábitos de navegación. Pueden ser los keyloggers, por ejemplo, que registran todo, a veces hasta cuando ni lo queremos.

• Por otro lado, el **adware** inunda nuestros dispositivos con anuncios molestos e incluso nos redirige a sitios inseguros. Un caso curioso fue “Fireball”, que, en 2017, afectó a millones de dispositivos.

• Y no olvidemos el **ransomware**, que cifra nuestros archivos y luego nos exige un rescate para liberarlos; “Ryuk” ha dejado su huella en grandes empresas y organismos gubernamentales.

Ahora, ¿cómo llega todo esto hasta nuestros sistemas?

Los correos de phishing suelen ser la puerta de entrada, donde mensajes engañosos nos incitan a descargar archivos dañinos.

También, basta que un USB o una red compartida se infecte y el contagio se extienda a otros equipos en la empresa.

No podemos bajar la guardia con software descargado de sitios poco confiables las aplicaciones pirata o supuestamente gratuitas a menudo vienen acompañadas de “regalos” indeseados.

Por último, si dejamos nuestros programas sin actualizar, abrimos la puerta a vulnerabilidades que los hackers pueden explotar sin mayores complicaciones.

¿Qué pasos sencillos podemos seguir para protegernos? La clave está en la rutina diaria y en actuar con cautela:

Asegurémonos de mantener todo actualizado, ya que esos parches suelen tapar fallos que los ciberdelincuentes buscan aprovechar.

Es vital usar contraseñas fuertes y, de ser posible, implementar autenticación multifactor para evitar accesos no autorizados.

Piénsalo dos veces antes de hacer clic en correos o enlaces que resulten sospechosos; confía en tu instinto.

Realizar copias de seguridad de forma regular nos asegura que, en caso de un ataque, siempre tengamos una red de apoyo para recuperar nuestra información.

Al trabajar fuera de la oficina, utiliza VPNs o conexiones seguras para proteger esos datos tan importantes.

Finalmente, es bueno capacitarnos en ciberseguridad cuanta más gente sepa identificar riesgos, mejor estaremos preparados.

En cuanto a las herramientas que nos respaldan, aquí algunos ejemplos útiles:

Antivirus como Bitdefender, Kaspersky o Windows Defender ayudan en la detección y eliminación de amenazas.

Los cortafuegos (por ejemplo, pfSense o Fortinet) se encargan de bloquear accesos no autorizados; funcionan como barreras vivas.

Programas anti-spyware y anti-adware (tipo Malwarebytes o AdwCleaner) nos ayudan a evitar seguimientos no deseados.

Herramientas contra el ransomware, como Acronis o RansomFree, se dedican a impedir cifrados maliciosos.

Y no menos importante, los sistemas para detectar intrusos (Snort, Suricata) nos dan esa alerta temprana cuando algo raro sucede en la red.

Conclusiones:

En resumen, la ciberseguridad es responsabilidad de todos y no se trata solo de contar con las mejores herramientas, sino de permanecer alertas y actuar con prudencia. De hecho, a partir de ahora, decidimos:

Realizar simulacros de phishing para que todos podamos aprender a reconocer esos mensajes engañosos.
Organizar una breve sesión de formación en ciberseguridad para afianzar nuestros conocimientos.
Revisar y reforzar nuestras políticas de seguridad; nadie debe relajarse en este aspecto.

Cuidémonos y mantengamos nuestra red segura, ya que, en el mundo digital, estar un poco más alerta nunca está de más.

Referencias

https://www.iebschool.com/blog/los-10-tipos-de-malware-mas-comunes-y-como-prevenirlos-tecnologia/?utm_source=chatgpt.com

https://nordvpn.com/es/blog/tipos-de-malware/?utm_source=chatgpt.com

https://blog.hackmetrix.com/10-herramientas-de-analisis-de-malware/?utm_source=chatgpt.com

https://nimbustech.es/ciberseguridad/mejores-herramientas-de-analisis-de-malware-empresas/

https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20241130.html

https://worldcampus.saintleo.edu/blog/cuales-son-las-mejores-herramientas-de-seguridad-informatica

https://www.iebschool.com/blog/los-10-tipos-de-malware-mas-comunes-y-como-prevenirlos-tecnologia/

https://blog.hubspot.es/website/que-es-seguridad-de-datos

https://www.avast.com/es-es/c-malware

https://www.docusign.com/es-mx/blog/desarrolladores/seguridad-informatica

https://thebridge.tech/blog/proteccion-contra-malware/