

Espionaje Industrial

Hoy la globalización y la modernización de los sistemas computacionales, permiten obtener información de la competencia, de las maneras más inverosímiles

Han existido casos, en que el robo de información ha hecho perder a industrias millones de dólares como por ejemplo sacar al mercado días antes, productos con el mismo nombre, o simplemente falsificar un invento a menor costo, copiando la fórmula de preparación, estrategias de fabricación, negociaciones millonarias, robo de patentes o contratos, etc., etc.

Este es un tema que se puede considerar como tabú dentro de cualquier organización, ya que implica muchos valores como son: la confianza, la responsabilidad, la moral, la seguridad, etc. de los cuales si no existen pruebas, sería difícil de responsabilizar.

Es por ello que sin el afán de escandalizar, es preferible saber cuales son algunos puntos donde a usted se le podría estar filtrando información

Riesgos con personal dentro de la empresa

Algo muy simple y vulnerable es el hecho de rastrear la basura, pero de fácil solución, utilizando una máquina de desintegración de la documentación desechada.

Otra manera muy común es tomar papeles de encima del escritorio o fax, o entrar al computador personal, siendo la solución el mantener los cajones con llaves y un protector de pantalla o simplemente cerrar la sesión cuando uno no se encuentra en su lugar de trabajo.

Otra actitud adecuada es llevar una trazabilidad de cada código de acceso, en sistemas de producción como son los sistemas Scada, tienen la opción de no tan sólo digitar una password sino también llevar un registro de las modificaciones o malos usos del sistema.

Existen softwares un poco más sofisticados, que logran capturar toda la actividad de los usuarios que utilizan un PC almacenando las teclas pulsadas en archivos log, también los hay que capturan imágenes de la pantalla cada cierta cantidad de tiempo, y almacenan en archivos de imagen y hasta de video, robando por ejemplo, información confidencial, password tipeados, fórmulas secretas, precios, sueldos, husmear conversaciones, revisar las páginas web visitadas, etc, etc. sin que el usuario ni siquiera lo imagine.

Control de acceso, cámaras de seguridad, acciones contra la intervención a los teléfonos, encriptación de la información enviada, almacenamiento de información en bases de datos y sistemas de respaldos remotos, son algunas de las buenas prácticas que se podrían implementar para resguardar la información con la que uno trabaja dentro de una compañía, pero ¿Qué sucede cuando el ataque es desde fuera de la empresa?

Riesgos desde fuera de la empresa

La seguridad de una empresa no es tan sólo una responsabilidad del área de informática, sino más bien una actitud de la institución completa, donde por ejemplo la secretaria podría ingresar un virus a su compañía con el simple hecho de responder una de estas decenas de cadenas que recibe diariamente y que solicitan que lo reenvíe a todos sus contactos, el riesgo es no tan sólo esparcir el virus sino también entregar su e-mail y el de sus conocidos para ser bombardeados con publicidad o más cadenas similares, donde la divulgación exponencial es inimaginable.

Existen también softwares microespías que almacenan pequeños archivos llamados "cookies" en nuestros computadores con el fin de robar información, que parecería inofensiva como es el número IP, el correo electrónico, páginas visitadas, etc, con el fin de enviar publicidad al e-mail robado.

La automatización industrial, las redes industriales, Internet y los computadores son recursos indispensables para la comunicación industrial. Transmitir datos a distancia hacen que los sistemas sean vulnerables en el aspecto de la seguridad y confiabilidad de la transmisión. Para intercambiar información por ejemplo de las oficinas centrales con alguna sucursal se tienen tres opciones:

Modem: Las desventajas es el costo de la llamada, por minuto conectado a larga distancia, además de calidad y velocidad no adecuadas.

Línea Privada: Se tendría que tender el cable ya sea de cobre o fibra óptica de un punto a otro, y si las distancias son de una región a otra el costo sería muy elevado. La ventaja de la fibra óptica es de no ser interceptable.

VPN: (Redes privadas virtuales) Los costos son bajos porque sólo se realizan llamadas locales, además de tener la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

Una práctica útil sería además implementar un "Firewall"; sistema que impone una política de seguridad entre la organización de red privada e Internet, el cual autoriza los servicios de red que pueden ser accedidos, así como también los usuarios. Desafortunadamente este sistema no puede ofrecer protección alguna una vez que el agresor traspasa la barrera de seguridad. Es por ello que muchas instituciones tienen por política no permitir el acceso de ningún tipo de "spam" y hasta de quitar las disqueteras con el fin de bloquear la mayor cantidad de puntos vulnerables.

Claro que esta situación no es propia de nuestras fronteras, sino que a nivel mundial, por ejemplo la mayoría de las llamadas y correos electrónicos que se realizan cada día son interceptados y analizados por una red de espionaje llamada "Echelon". El espionaje industrial es una de las "prioridades" encomendadas a la CIA desde hace décadas.

Todos estamos de acuerdo en que en este ámbito no se puede hablar de seguridad al 100%, más aún cuando las empresas no son conscientes del riesgo real al que están expuestas. Vivimos bajo una falsa sensación de seguridad. Pero lo alentador es que el espionaje puede ser prevenido. ¿Tomó Ud. los resguardos necesarios?

Por Lucía Pinto Jonas, de Control & Logic.
Miembro del Comité de Automatización y Control Industrial de AIE;
lpinto@controlandlogic.cl - www.aie.cl