¿Qué tan seguro es su sistema de control?

No se tiene imagen, favor de agregar una referente al tema

-Maroochydore, Australia, abril de 2000 - Despedido por el contratista que instaló el sistema de control de la planta de tratamiento de agua local, el ingeniero Vitek Boden fue rechazado por un trabajo por el ayuntamiento. Despedido y criticado, Boden buscó su venganza cruel. Usando una laptop robada y un radio de dos vías, conectó de forma inalámbrica al sistema de control de la planta y emitió unas pocas líneas de código. En el transcurso de varias semanas, presidió la liberación de cientos de miles de galones de aguas negras en vías acuáticas cercanas.

-Davis, Ohio, enero de 2003 - El equipo de proceso de la planta de alimentación nuclear de Davis-Besse y el sistema de visualización de parámetros de seguridad se apagaron durante varias horas. ¿El culpable? El gusano Slammer, inadvertidamente liberado por un contratista que estableció una conexión de computadora sin protección a la red corporativa, a través de la cual el gusano llegó a la red de la planta y el servidor SQL. Sobre la investigación, Davis-Besse descubrió que los ingenieros de la planta ni siquiera eran conscientes del parche Microsoft liberado seis meses antes. Afortunadamente, la planta estaba fuera de línea, por lo que ninguno de los sistemas afectados causó fallas de seguridad.

¿Cuál es el hilo común que conecta estos dos ejemplos? No es el hecho de actuar después ocurridos los hechos, si no la falta de prevención antes de tiempo para evitar que sucedan. En la primera situación, la capacidad de Boden para iniciar sesión en el sistema debió cerrar en el momento en que su posición fue terminada. En este último caso, los parches de seguridad de Windows no fueron instalados cuando fueron emitidos. A pesar de que el servidor SQL de planta no se haya unido permanentemente al sistema de la empresa, los parches y actualizaciones del sistema operativo (OS) deberían haber sido aplicadas en caso de incumplimiento.

Si usted tiene un pequeño sistema industrial de E/S que forma las entrañas de una máquina envasadora, una adquisición de datos y un sistema de control para una planta piloto, un sistema de control basado en PC/PLC, o un sistema de control distribuido, usted no puede permitirse correr riesgos con la seguridad. Los hackers que se empeñan en la destrucción total pueden sorprenderle con su conocimiento de redes y programas de PLC/DCS. Y sólo porque usted puede tener un PLC o DCS propios, o ejecutar una máquina Linux o UNIX, no está garantizada la seguridad a menos que usted tome algunas medidas iniciales. Como primera línea de defensa es necesario saber de dónde están viniendo los ataques.

El empleado descontento

Clarence es el "modelo" de los empleados. Leal, cortés, un solucionador de problemas astuto, paciente, eficiente e innovador. Pero lo despiden por reducción de personal o externalización y podría ser una amenaza a la seguridad. ¿Qué pasa si el departamento de IT elimina su casilla de correo electrónico de forma casi instantánea con su despido, pero nadie piensa en quitar el inicio de sesión de FTP, eliminar su inicio de sesión TELNET al sistema de adquisición de datos, apagar su conexión VPN, y eliminar su marcación remota? ¿Qué pasa con la conexión inalámbrica? ¿Ha sido asegurado? Usted no tiene que proporcionar los puntos de conflicto para los empleados descontentos. Dejemos que Starbucks® lo haga.

Una vez que haya removido a Clarence de todos los inicios de sesión posibles y bases de datos, asegúrese de que su "fantasma" no regrese a través de una copia de seguridad/restauración. Compruebe que su inicio de sesión también haya sido removido de cualquier archivo. Y tenga en cuenta que el 70% de los incidentes cibernéticos industriales se originan desde el interior de la empresa.

El hacker implacable

"Ha sido una semana tranquila en el lago Wobegon". Tal vez, pero en internet, semanas tranquilas sin los hackers y los virus que crean son un recuerdo borroso. Esté o no su planta atada en la red LAN de la empresa, es una buena idea tener protección antivirus en todos los equipos, a menos que, por supuesto, usted tenga un sistema integrado que no esté expuesto a la red. En una semana puede haber tres o cuatro actualizaciones de definición de virus McAfee® para combatir diversas versiones de gusanos MyDoom y Bagle.

Si bien no todos los virus o gusanos destruirán sus datos, pueden robar información sensible que es probable usted no quiere que tengan. Suponiendo que no hacen daño a su computadora y no roban datos, los gusanos pueden disminuir el ancho de banda de la red al mínimo, y eso es lo que cerró la planta de Davis-Besse durante unas seis horas. Una vez infectado por correo electrónico, una computadora con un gusano propaga sus gérmenes desagradables a otras computadoras en su red entre iguales, y a otras computadoras de todo el mundo a través de correo electrónico. Sus computadoras se convierten en zombies, y cuando son comandadas por un hacker, se unen a un ejército de computadoras dirigiendo rechazo de ataques de servicio contra un destino previsto, por ejemplo, Microsoft®.

No es un virus, pero casi tan malo

Si una planta, conectada a internet Pentium de repente funciona a 25 MHz 386, es posible que tenga una infección, o si este equipo también se utiliza para navegar por la Web, y permite instalaciones descargables, la extrema lentitud puede deberse a adware , spyware, u otros troyanos no deseados. Algunos sitios Web que agregan barras de herramientas en sus navegadores pueden instalar hasta tres o cuatro programas o servicios que hacen un seguimiento de todos tus movimientos en internet y transmiten la información a las empresas de marketing. Si

bien estos no son técnicamente virus, pueden tener el mismo efecto en su máquina - lo atoran a paso de tortuga. A veces, estos programas le darán una advertencia sobre lo que van a instalar, pero por lo general está enterrado en un par de miles de palabras del texto repetitivo. A veces, si tiene suerte, van a aparecer en "Add-Remove Programs", donde usted puede deshacerse de ellos.

¿Cómo evitar problemas?

Evite conectar el HMI o computadora de control a la red y no conecte una línea telefónica para acceso remoto. Si bien es necesaria, y su planta LAN y LAN de la empresa están unidas, háblelo con el IT, y asegúrese de que al menos tengan routers/firewalls intermedios para controlar el tráfico, por lo que sólo los hosts específicos llegan a comunicarse con el sistema de piso de la planta. Las redes de la planta se pueden poner en subredes separadas, lo que proporciona un cierto aislamiento. Use routers para cerrar los puertos innecesarios y firewalls para excluir los hosts y dominios.

Utilice sólo las versiones "profesionales" de Windows. Si usted todavía tiene Windows NT flotando alrededor, no espere que Microsoft apoye mucho más tiempo. Aunque es molesto soportar frecuentes actualizaciones de Windows (especialmente para servidores porque nunca hay un buen momento para reiniciar el servidor después de instalar la actualización), si no se ha actualizado recientemente, vas a incitar problemas. Es probablemente una buena idea consultar con proveedor de software DAQ o HMI antes de aplicar actualizaciones, por si acaso hay algún problema. Las actualizaciones también significan "Service Packs", que son hasta la versión 4 en Windows 2000 y la versión 2 (próxima a estrenarse) en Windows XP.

Si un HMI (Human Machine Interface) debe estar conectado a internet, la protección antivirus es obligatoria, y es posible que también desee considerar el uso de Spybot Search & Destroy®, Ad-aware® o herramientas similares para buscar y eliminar cualquier spyware/adware comercial que pueda existir en el equipo. Comprobando la lista de tareas y ejecutando un programa sniffer (como ActivePorts®) es una buena manera de ver lo que está pasando detrás de las escenas, y lo que podría estar afectando su rendimiento. Tomar una instantánea de la lista de tareas [ALT-Impr Pant], pegarlo en un documento de Word, e imprimirlo. Revise su lista de tareas regularmente para ver si hay "nuevas" tareas no autorizadas o programas ejecutándose, lo que podría ser virus, spyware, adware, etc.

Una buena manera de evitar que spyware y adware sean instalados es asegurarse que las cuentas de usuario no tienen los privilegios de instalación. No les dé a los operadores más privilegios de los necesarios para conseguir su trabajo hecho. Si tiene que usar Internet Explorer, mantenga la configuración de seguridad muy alta. Probablemente no sea una buena idea mezclar e-mail con HMI, pero si debe tener e-mail, ¿por qué no intentar con un cliente más débilmente conectado, como Pegasus® o Eudora® en lugar de Outlook® o Outlook Express?

Tenga cuidado con el supuesto de que los sistemas integrados son seguros. En agosto de 2003, varios cajeros automáticos Diebold ejecutando Windows XP Embedded fueron apagados debido a una vulnerabilidad RPC DCOM Windows XP Embedded, que fue atacada por Nachi, un

descendiente del gusano Blaster. Formas de prevenir la infección incluyen mantenerse al día con los parches de Microsoft, instalar sólo los módulos necesarios para una aplicación, el cierre de todos los puertos innecesarios, y el cierre de cualquiera de los servicios que no sean necesarios, especialmente RPC. Además, un firewall configurado y correctamente colocado puede ayudar. Si usted está diseñando un sistema integrado desde el principio, una forma de eliminar a los gusanos que se ejecutan en sistemas basados en Microsoft es no utilizando un sistema operativo de Windows. En su lugar, ¿por qué no mirar en QNX®, Wind River®, o un sabor de un sistema operativo Linux® en tiempo real?

Conclusión

En los "viejos tiempos" las computadoras obtenían virus de los usuarios intercambiando disquetes infectados. El tiempo que tardó en propagarse era muy lento en comparación con computadoras conectadas a internet de hoy en día donde los virus viajan alrededor del mundo varias veces en menos de una hora. Ahora usted puede conseguir un virus de computadora con sólo estar conectado a internet. El mejor remedio es estar al día con los parches de software y actualizaciones de definición de virus, y cerrar todos los servicios de Windows que no necesita. Lo mismo se aplica si se está ejecutando Linux/UNIX. Para obtener más información, vea la barra lateral "Ayuda e información de seguridad". Y, por cierto, piense dos veces antes de despedir a Clarence.

Para cualquier duda o comentario escribir a sgarza@sdindustrial.com.mx