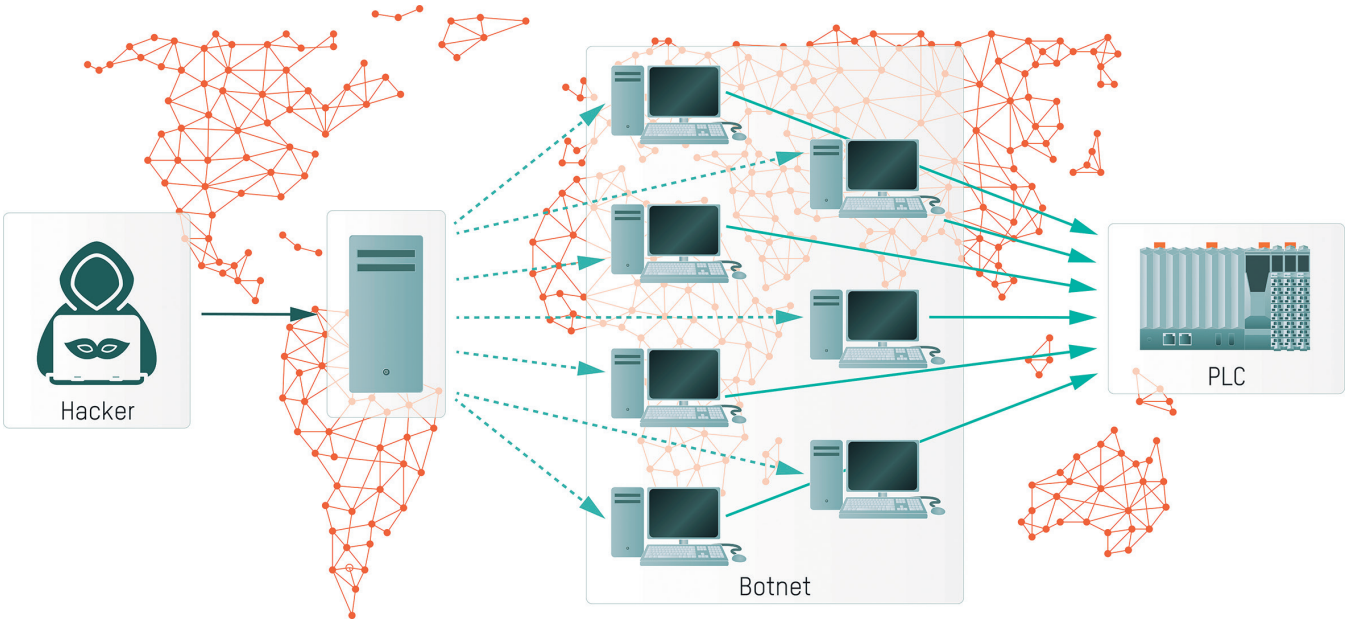
Ciberseguridad para controles

Carmen Klingler-Deiseroth
Periodista

FIGURA 1. En un ataque DDoS, un *hacker* distribuye programas a través de un *botnet* para realizar un ataque concertado que paraliza un control



La transferencia de datos desde el control de la máquina a la nube requiere de una conexión a Internet. Ello, no obstante, los hace susceptibles a los ciberataques. Por lo tanto, las máquinas con conectividad en la nube necesitan protección especial.

Antes de la Internet industrial de las cosas (IoT industrial), los controles de máquinas se comunicaban, si es que lo hacían, solo entre sí o con sistemas de nivel superior dentro de la red de la compañía. Una conexión directa a Internet era algo poco habitual. Los fabricantes de máquinas y sus operarios no tenían motivos para preocuparse por el tema de la ciberseguridad. Pero eso está cambiando, explica Andreas Hager, director de Productos de B&R para sistemas de control. En las soluciones de la IoT industrial, se utilizan PC industriales y otro tipo de hardware como dispositivos Edge con una conexión directa a Internet. Esto los hace vulnerables como posibles objetivos para los *hackers* informáticos (Figura 1).

ATAQUES DDOS

Los *hackers* pueden paralizar los controles y, por lo tanto, máquinas enteras, por ejemplo, al colapsarlos con tráfico. Esto se conoce como ataque

DDoS (denegación de servicio distribuida, por sus siglas en inglés): Un *hacker* distribuye programas de ataque a través de la llamada *botnet* (red de bots), que comprende varios cientos de miles de ordenadores, smartphones y tabletas, convirtiéndolos en armas activas. A una orden, estos *bots* bombardean un control de máquina con tantas solicitudes simultáneas que provoca su fallo por carga excesiva, y la máquina se detiene, como lo demostró recientemente un ataque de *malware* realizado contra un fabricante de microprocesadores.

PUERTOS ABIERTOS

Para transferir datos a la nube, los puertos deben abrirse en el control de la máquina. "*Mientras el canal de comunicación entre el control y la puerta de enlace en la nube esté abierto, estos puertos son una ventana de acceso para los hackers*", explica Hager. Sin embargo, ese no es el único problema. Los dispositivos que están conectados directamente a Internet deben actualizarse periódicamente para cerrar las brechas de seguridad que se van descubriendo.

"*Muchas máquinas funcionan durante semanas o meses*", señala Hager. Sin embargo, las actualizaciones solo se pueden instalar cuando la máquina está detenida. Después de una actualización, es posible que incluso sea necesario ajustar la aplicación. "*Eso es mucho trabajo y, a la larga, simplemente no es una respuesta viable*", añade.

Afortunadamente, hay una solución simple: la funcionalidad de control y la funcionalidad de comunicación deben estar aisladas la una de la otra. De esa forma, un ataque DDoS no podría ser lo suficientemente profundo como para afectar al control de la máquina. "*En el peor de los casos, puede perder la comunicación con la nube, pero la máquina en sí misma puede seguir funcionando*", enfatiza Hager (Figura 2).

B&R ha presentado el SiteManager con esta finalidad. El dispositivo tiene un *firewall* integrado y realiza todas las tareas necesarias para la ciberseguridad, como mantener actualizados los certificados en la nube y aplicar parches para cerrar los agujeros de seguridad (Figura 3).

FIGURA 2. El SiteManager transfiere datos a la nube de forma segura

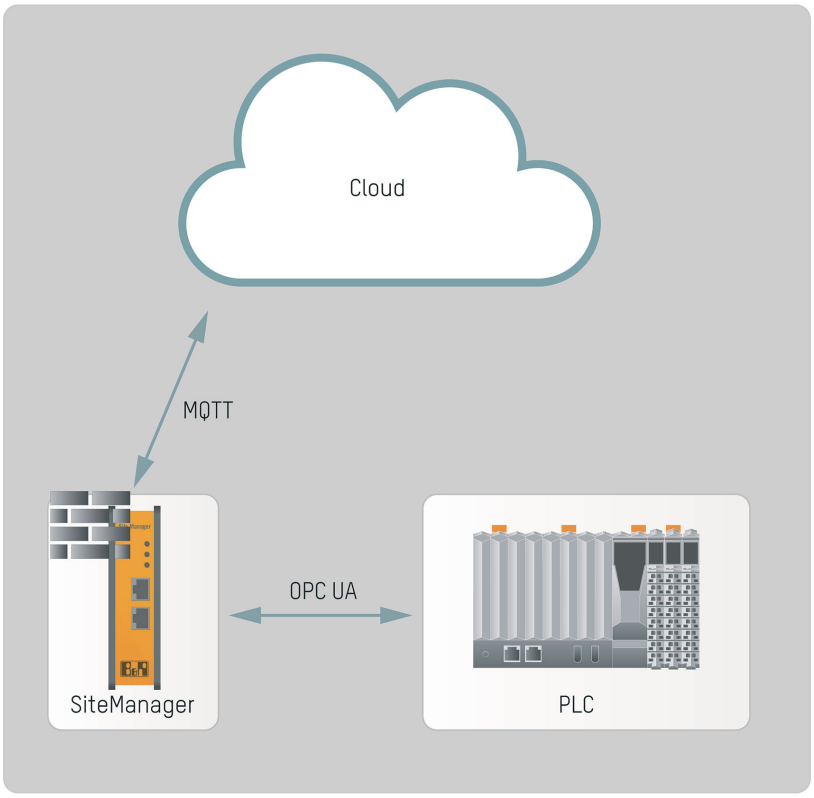


FIGURA 3. El SiteManager de B&R está disponible en tres variantes, proporcionando una conexión a Internet a través de LAN, WLAN o red móvil

CONECTIVIDAD CON LA NUBE

Para transferir datos a la nube, el control se conecta con el SiteManager a través de OPC UA. Durante la configuración, el usuario define qué datos son los que se van a transferir. También es posible transferir diferentes datos a diferentes proveedores de la nube. La configuración es una simple cuestión de marcar casillas en la interfaz de usuario basada en la web del SiteManager.

Si se necesita actualizar un certificado en la nube, el operario de la máquina no tiene que hacer nada.

FIGURA 4. B&R Hypervisor posibilita el uso simultáneo de un PC industrial como control de máquina y como SiteManager integrado. No se requiere ningún software adicional

» Si se necesita actualizar un certificado en la nube, el operario de la máquina no tiene que hacer nada. SiteManager descarga e instala automáticamente las actualizaciones sin afectar el funcionamiento de la máquina

Andreas Hager, director de Productos - Sistemas de Control, B&R

SiteManager descarga e instala automáticamente las actualizaciones sin afectar el funcionamiento de la máquina. Esto también garantiza que siempre se cumplan las directrices de seguridad de los proveedores de la nube, y que cualquier brecha de seguridad potencial sea rápidamente cerrada. "*El hecho de tener el SiteManager entre el control y la nube garantiza que la transferencia de datos entre la máquina y las aplicaciones fuera de la red de la compañía estén protegidos contra accesos no autorizados*" (Figura 4).

MANTENIMIENTO REMOTO SEGURO

"*Los requisitos de seguridad para el mantenimiento remoto son muy similares a los de la comunicación en la nube*", explica Hager. El SiteManager, por lo tanto, también es perfectamente adecuado para este propósito.

El dispositivo permite a los técnicos de servicio conectarse al sistema de control de la máquina a través de una conexión VPN segura y buscar errores. Un sistema de gestión de usuarios proporciona un control claramente definido y a prueba de manipulaciones sobre qué técnicos tienen acceso a qué controles. "*Con un técnico en las instalaciones, se puede iniciar un proceso de diagnóstico de errores específico*", asegura Hager. "*SiteManager garantiza que la transferencia de datos entre la máquina y las aplicaciones fuera de la red de la compañía queden protegidos contra accesos no autorizados y ciberataques*".