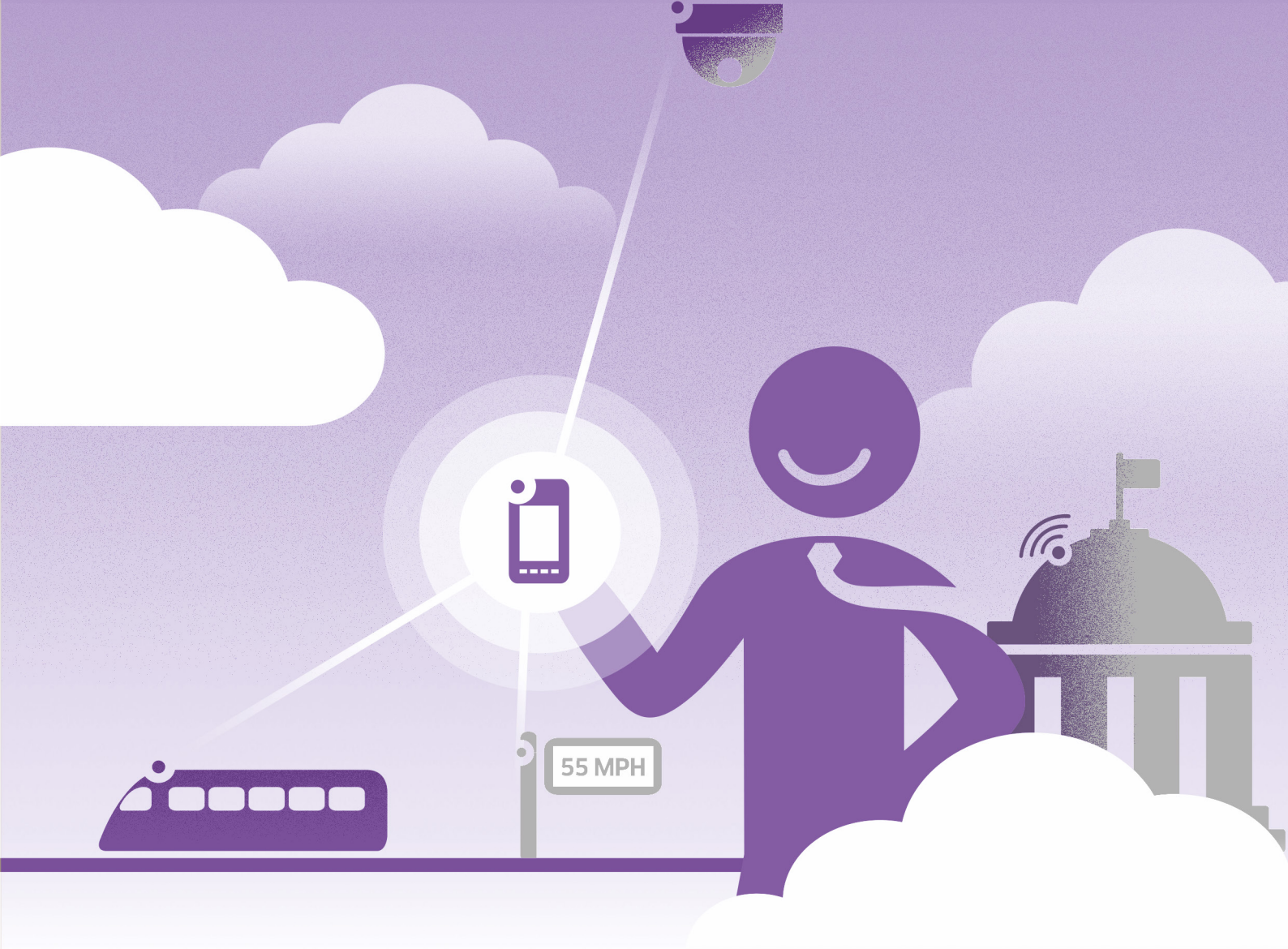


Internet de las Cosas para la Administración Pública

Constituya una base segura para aprovechar IoT en la mejora de los servicios públicos, una infraestructura más inteligente, y una mayor habitabilidad y seguridad

Informe de la solución
IoT en la Administración Pública

Alcatel·Lucent
Enterprise

IoT cambia fundamentalmente la ecuación de la Administración Pública

Internet de las Cosas (Internet of Things, IoT) tiene potencial para transformar el sector público ya que altera profundamente la forma que tienen los organismos públicos de recoger los datos y la información al combinar las principales tendencias técnicas y de negocio de movilidad, automatización y análisis de datos. IoT recurre a redes de objetos físicos mediante el uso de sensores embebidos, actuadores y otros dispositivos que captan y transmiten información sobre la actividad de la red en tiempo real. Los datos recogidos por estos dispositivos son analizados por los empleados públicos para:

- Conectar mejor a ciudadanos y organismos públicos para proporcionar servicios de alta calidad, seguros y eficaces, así como recursos que mejoren la colaboración y la confianza entre las Administraciones y la población que atienden, aumentando para ello la habitabilidad, la operatividad y la sostenibilidad.
- Aumentar la seguridad de los ciudadanos mediante un mejor conocimiento de las operaciones de los sistemas de la ciudad a través de los datos de sensores que efectúan un seguimiento total de las anomalías en las velocidades de los trenes, las temperaturas de las carreteras y la localización en tiempo real de los autobuses urbanos.
- Reducir la congestión y el uso de la energía mediante las tecnologías de la Ciudad Inteligente que aprovechan los datos en tiempo real para mejorar el dimensionamiento de los recursos en función de la demanda; y proporcionar la agilidad necesaria para reaccionar con rapidez a las condiciones del tráfico, a las variaciones del consumo de agua o de electricidad o a cambios en la calidad del aire.
- Mejorar el rendimiento operativo y el mantenimiento mediante la supervisión proactiva de la infraestructura pública crítica y la creación de procesos más eficientes para reducir los costes operativos y mejorar la capacidad del sistema.
- Mejorar la seguridad pública al responder a las emergencias de forma más rápida y efectiva.

Posibilidades de IoT para la Administración Pública

Las soluciones IoT prometen lograr que las organizaciones del sector público sean más inteligentes y más exitosas. IoT protagoniza las fuerzas que impulsan a los organismos públicos a proporcionar mejores servicios, la seguridad, un transporte eficiente, infraestructuras públicas más inteligentes, y una gestión estratégica del tráfico. Estos son algunos ejemplos de IoT en la Administración Pública:

- Transporte público más eficiente y más rentable, que emplee una red de sensores, cámaras digitales y vehículos conectados para aumentar la capacidad del sistema, así como para mejorar la seguridad y la comodidad de los viajeros, reduciendo al mismo tiempo los costes y los riesgos.
- Soluciones de vídeovigilancia formadas por cámaras de alta resolución en circuito cerrado para aumentar la seguridad del transporte público y la infraestructura de la ciudad, supervisar el movimiento de personas y multitudes, y facilitar respuestas de emergencia. El software para análisis de vídeo inteligente puede automatizar la detección temprana de comportamientos sospechosos y equipaje abandonado.
- Paneles con mensajes dinámicos para que visualizando para ello en tiempo real el estado del tráfico, carriles cerrados y tiempos de desplazamiento recibidos automáticamente desde sensores y cámaras.
- Soluciones energéticas inteligentes que supervisan el consumo eléctrico y crean sistemas energéticos más robustos que reducen el consumo y menos emisiones relacionadas con la energía con el fin de mejorar la eficiencia y la sostenibilidad energética a escala municipal.

Desafíos del despliegue de IoT

IoT aporta un flujo de datos sin precedentes, lo cual genera desafíos en cuanto a prestaciones, operativos y de gestión a la infraestructura de la red, así como mayores riesgos de seguridad desde todos los puntos. Para solucionar estas cuestiones, los organismos públicos necesitan adaptar los diseños de la red tradicional para ofrecer nuevos niveles de inteligencia, automatización y seguridad a la red.

Las organización públicas necesitan una infraestructura de red económica que garantice el manejo de enormes flujos de datos, además de ser fácil de gestionar. La infraestructura debe:

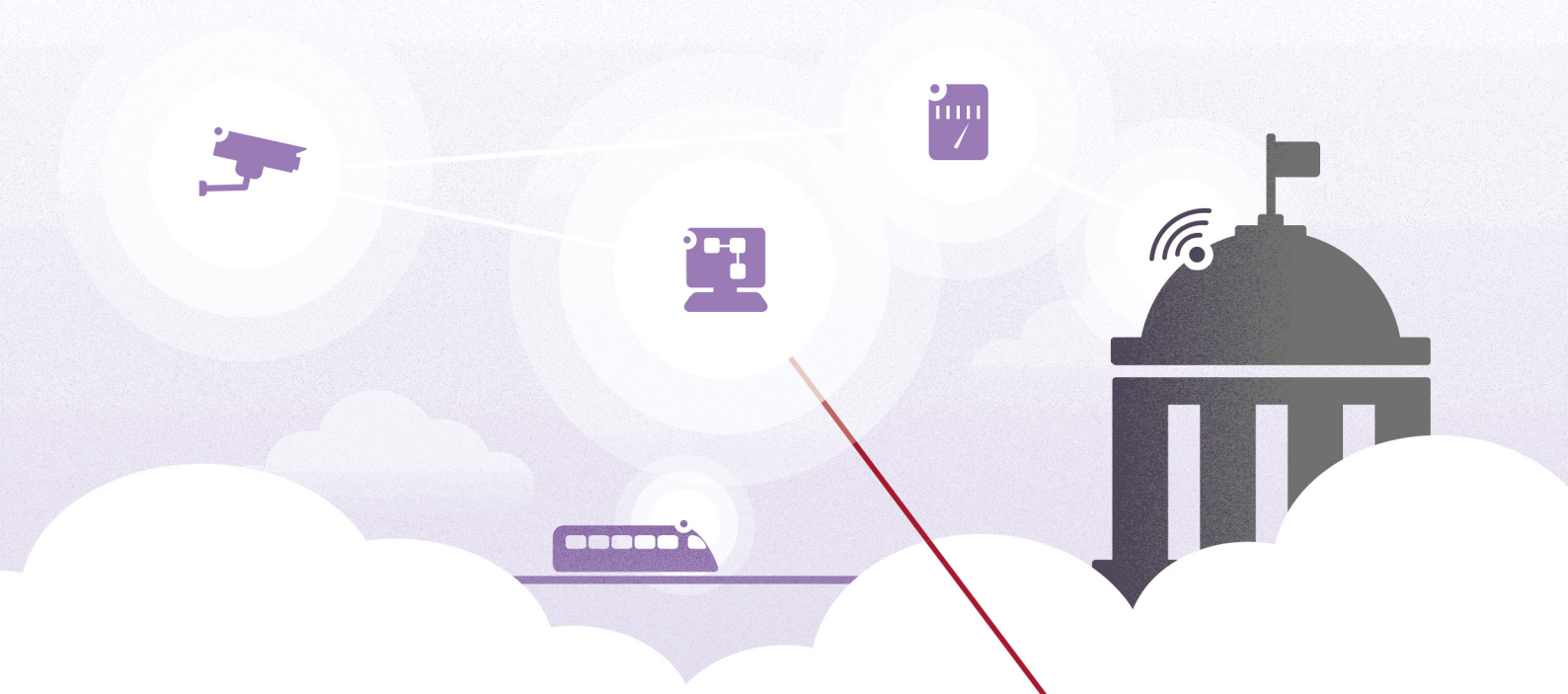
- Ofrecer un proceso sencillo y automatizado para la incorporación de dispositivos IoT. Los grandes sistemas IoT contienen miles de dispositivos o sensores, y el suministro y la gestión manual de todos estos puntos aumenta la complejidad y la posibilidad de errores. La incorporación automatizada permite que la infraestructura de la red reconozca los dispositivos dinámicamente, así como asignarlos a la red segura más apropiada.
- Suministrar los recursos correctos a la red para que el sistema IoT funcione de manera adecuada y eficiente. Muchos dispositivos en el sistema IoT aportan información crítica que exige un determinado nivel de calidad del servicio. Por ejemplo, en algunos casos es preciso reservar el ancho de banda adecuado en una infraestructura de red de altas prestaciones para garantizar el rendimiento y la fiabilidad del servicio.
- Proporcionar un entorno seguro frente a ciberataques y pérdida de datos.Debido a que los numerosos dispositivos y sensores de la red IoT de la Administración conllevan un gran número de vectores de ataque potencial, la seguridad es fundamental para aminorar los riesgos de cibercrimen. La seguridad es necesaria a múltiples niveles, incluyendo el confinamiento de las propias redes IoT.

Los profesionales de TI tienen previsto potenciar IoT

Los profesionales de TI en diversos sectores ya tienen previsto potenciar el uso de soluciones IoT en el próximo futuro. De acuerdo con el estudio realizado en 2017 por 451 Research sobre Internet de las Cosas, el 67% de los profesionales de TI que respondieron al cuestionario dijeron que sus organizaciones ya han instalado una solución IoT, o bien que tenían un sistema IoT en fase piloto. Un 21% por ciento de las personas que respondieron al cuestionario afirmaron que sus organizaciones tienen previsto instalar soluciones IoT durante los próximos 12 meses y un 11% indicó que tenían prevista la implementación de IoT dentro de más de un año.

IoT aumenta la exposición de la Administración Pública a los ciberdelitos

El crecimiento de IoT en el sector público también conlleva una explosión de las amenazas de ciberseguridad ya que la proliferación de sensores y dispositivos conectados aumenta enormemente el número de puntos de entrada para ataques a la red. IoT es especialmente susceptible ya que muchos dispositivos IoT se fabrican sin tener en cuenta la seguridad, o bien son construidos por empresas que no comprenden los actuales requisitos de seguridad. En consecuencia, los sistemas IoT se han ido convirtiendo en el eslabón débil para la seguridad en las redes de la Administración.



- El ataque del ransomware WannaCry en mayo de 2017, perpetrado en redes públicas de todo el mundo, encriptó los datos y paralizó los ordenadores durante días en el Ministerio del Interior de la Federación Rusa, el Ministerio de Asuntos Exteriores de Rumanía, y en los gobiernos de cuatro estados de la India.[1]
- En marzo de 2018, el gobierno municipal de Atlanta se vio gravemente afectado por un ataque de ransomware que aprovechó las vulnerabilidades de la red de la Ciudad Inteligente y de los archivos encriptados de la Administración, bloqueó el acceso a los servicios en línea (incluyendo el correo electrónico) y bloqueó el funcionamiento de los juzgados.[2]

La Administración Sueca de Transporte (Trafikverket) se vio afectada en 2017 por un ataque de denegación de servicio distribuido (distributed denial of service, DDoS) que puso fuera de servicio el sistema automático que gestiona los trenes, así como la red de correo electrónico y de comunicación de este organismo, en perjuicio de los viajeros ferroviarios en todo el país, que no podían recibir información sobre lo que estaba ocurriendo.[3]

Construcción de una infraestructura segura de la red IoT

La protección del tráfico y de los dispositivos IoT es un desafío que no se puede superar con una sola tecnología de seguridad. Exige un enfoque estratégico que aproveche diversas protecciones de seguridad.

Para ayudar a las organizaciones a aprovechar las ventajas y a mitigar los riesgos de la implantación de IoT, Alcatel-Lucent Enterprise (ALE) proporciona una estrategia de seguridad multinivel. La estrategia de ALE ofrece protección en cada capa de la infraestructura, desde cada usuario y cada dispositivo hasta la propia capa de la red. También proporciona una estrategia de confinamiento de IoT para simplificar y proteger la incorporación de dispositivos y suministrar los recursos adecuados a la red para el funcionamiento correcto y eficiente del sistema, todo ello en un entorno seguro que proteja los sistemas de la Administración frente a ciberataques.

Confinamiento de IoT

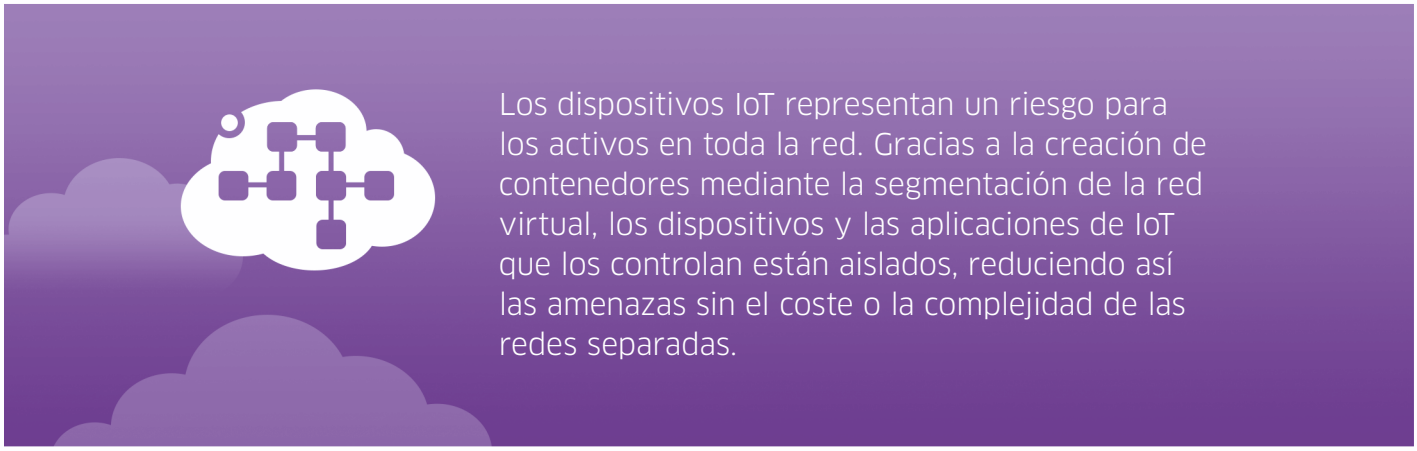
Para permitir el confinamiento de IoT, todos los usuarios, dispositivos y aplicaciones de la red de ALE son perfiles asignados. Estos perfiles, que definen funciones, autorizaciones de acceso, niveles de calidad de servicio y otro tipo de información relacionada, se transmite a todos los conmutadores y puntos de acceso de la red.

- Los dispositivos se encuentran en “contenedores virtuales” que aplican técnicas de virtualización de la red, de manera que diversos dispositivos y redes pueden utilizar la misma infraestructura física mientras permanecen aislados del resto de la red.
- En estos contenedores virtuales se aplican normas de calidad de servicio y seguridad.
- Al dividir la red mediante contenedores virtuales, si se produce una brecha en una parte de la red virtual ello no afecta a otros dispositivos o aplicaciones en otras redes virtuales.
- Cuando se conecta un nuevo dispositivo IoT, la red reconoce automáticamente su perfil y asigna al dispositivo en entorno virtual apropiado.
- La comunicación se limita a los dispositivos de este entorno virtual y a la aplicación en el centro de datos que controla estos dispositivos.
- Debido a que todos los usuarios tienen perfiles dentro de la red de ALE, el acceso a los contenedores virtuales de IoT se puede limitar a las personas y grupos autorizados.

Máxima seguridad

Además del confinamiento de IoT, las tecnologías de la red de ALE proporcionan seguridad por capas en varios niveles de la red.

- Al nivel del usuario, los perfiles aseguran que los usuarios obtengan la autenticación y autorización con los derechos de acceso apropiados.
- Al nivel del dispositivo, la red asegura que los dispositivos tengan autenticación y cumplan las normas seguridad establecidas.
- Al nivel de la aplicación, la red establece normas relativas a cada aplicación o grupo de aplicaciones, como bloqueo, máximo ancho de banda y control de quién accede a cada aplicación.
- Al nivel de la red, los conmutadores de ALE aprovechan las ventajas de un código diversificado y seguro. Este protege las redes frente a vulnerabilidades intrínsecas, código oculto, malware embebido y potenciales puertas traseras que puedan afectar a conmutadores, enrutadores y otro hardware de misión crítica.
- El análisis inteligente de ALE utiliza inspección avanzada de paquetes y otras tecnologías para detectar el tipo de datos y aplicaciones que se mueven por la red, posibilitando así la identificación de patrones inusuales y accesos no autorizados.



Gestión operativa y de la red de extremo a extremo

Las soluciones de ALE para redes también ofrecen ventajas significativas de tipo operativo y para su gestión.

- ALE permite el funcionamiento de varias redes virtuales separadas como una sola infraestructura, lo cual supone un ahorro en el gasto de capital en varias redes físicas.
- La solución de acceso unificado de ALE permite el funcionamiento conjunto de redes cableadas e inalámbricas como una sola red robusta, con un conjunto común de servicios de red, un marco normativo común, una técnica común de autenticación y una sola base de datos de autenticación.
- Las soluciones de ALE para redes también tienen un solo sistema de gestión para todos los elementos de la infraestructura, incluyendo la gestión unificada de redes LAN y WLAN. El paquete de gestión Alcatel-Lucent OmniVista® 2500 proporciona un solo panel para gestionar entornos virtuales, conmutadores, puntos de acceso y otros componentes de la red.

Gama para redes de altas prestaciones

Los conmutadores, puntos de acceso y controladores de ALE ofrecen capacidades de elevado ancho de banda y baja latencia y pueden gestionar un gran número de dispositivos en entornos de alta densidad. Los productos y soluciones para redes de ALE pueden cubrir las necesidades de instalaciones de cualquier tamaño. ALE también suministra una selección de conmutadores, puntos de acceso y enrutadores robustos para el despliegue de redes en el exterior o en entornos adversos.

Ya están aquí las redes y las estrategias para una IoT segura en la Administración

Los productos y soluciones de ALE constituyen la base de una red segura para ayudar a los organismos públicos a instalar sistemas IoT que mejoren la conexión entre ciudadanos y servicios, permitan soluciones para la Ciudad Inteligente y mejoren la eficiencia operativa de la infraestructura pública, además de reducir costes y riesgos. El confinamiento de IoT de ALE y las estrategias de seguridad por capas simplifican la configuración de redes IoT en la Administración al facilitar la incorporación de dispositivos, proporcionando así un funcionamiento más eficiente y una enorme mejora de la seguridad. ALE ayuda a los organismos públicos a aprovechar al máximo las ventajas de IoT a través de mayores niveles de inteligencia, automatización y seguridad de la red.

¿Desea más información?

Para más información sobre las soluciones IoT de ALE, visite Seguridad de IoT de ALE.

Administración conectada

Le ayudamos a conectar sus comunidades suministrándole una tecnología que funciona, para toda su organización y para las personas a las que atiende. Con una cobertura global y un enfoque local, suministramos redes y comunicaciones para ofrecer movilidad, seguridad y protección a los organismos públicos.

[1] WannaCry Ransomware Attack

[2] A Cyberattack Hobbles Atlanta, and Security Experts Shudder

[3] DDoS Attack Halts Swedish Transport Systems