Microsoft

DESARROLLANDO UNA ESTRATEGIA CIUDADANA

SEGURIDAD CIBERNETICA

Una guía de siete pasos para gobiernos locales

CRISTIN FLYNN GOODWIN
J. PAUL NICHOLAS
Octubre de 2014

CONTENIDO

Introducción

Las ciudades actuales son centros vibrantes de vida y economía modernas, cada vez más dependientes de las tecnologías de la información y la comunicación (TIC).

Junto con el crecimiento del valor económico de las TIC para las ciudades, crecen rápidamente también las amenazas. En este ambiente de seguridad, una estrategia para proteger la seguridad cibernética de una ciudad es crítica para gestionar los riesgos y aumentar la resiliencia. Una ciudad segura puede confiar en estar mejor posicionada para aprovechar las oportunidades y crecer.

A nivel nacional, las autoridades lidian con principios, leyes, políticas y programas para mejorar la seguridad cibernética. Las ciudades se están convirtiendo en parte crucial de esta discusión porque son blanco también de ataques informáticos. Las ciudades tienen necesidades de seguridad práctica que no pueden esperar por políticas nacionales e internacionales para seguir el paso. Necesitan formas inmediatas para priorizar los riesgos y asignar roles y responsabilidades en aspectos clave de la seguridad cibernética. Además, las ciudades tienen que equilibrar costos, sistemas existentes y heredados y la administración de programas y sistemas nuevos. Una estrategia de seguridad cibernética local puede ayudar a una ciudad a empezar.

Microsoft tiene años de experiencia en el tratamiento de amenazas en el ciberespacio mundial. Por ejemplo, cada mes la compañía recibe información de amenazas de más de 600 millones de sistemas en más de 100 países y regiones. Recopilar este vasto conocimiento de amenazas, junto con la vasta experiencia de la compañía trabajando con gobiernos en busca de soluciones a los desafíos de la seguridad cibernética, Microsoft ha creado un enfoque de principios de siete pasos para ayudar a las ciudades a diseñar e implementar estrategias de seguridad cibernética que se adapten a otros programas urbanos transformativos orientados a aumentar la resiliencia:

1. Construir un enfoque a la seguridad cibernética basado en los riesgos
2. Establecer prioridades claras
3. Definir los lineamientos de seguridad TIC mínimos
4. Compartir y coordinar información sobre amenazas y vulnerabilidades
5. Construir capacidad de respuesta a incidentes
6. Fomento de la concientización pública, educación y entrenamiento de la fuerza laboral
7. Facilitar la cooperación pública, privada y académica

Evolución de un mundo de ciudades conectadas

Beneficios de la nube

Con su arquitectura flexible y escalable, informática basada en la nube ayuda a aumentar la eficiencia de la ciudad y la calidad del servicio, al tiempo que apoya su participación en la economía global.

La nube puede ayudar a las ciudades:

- Aumenta la resiliencia. Por medio del almacenamiento centralizado de datos, gestión y respaldo, la recuperación de datos en respuesta a interrupciones locales puede ser más fácil y rápida.
- Incrementa la eficiencia. Los servicios de la nube pueden ajustarse, de ser necesario, para mejorar la eficiencia operativa.
- Simplifica operaciones. La nube puede ayudar a optimizar instalaciones y reducir los requerimientos de gestión TIC.
- Provee mejores servicios a la ciudadanía. Nuevos servicios innovadores son posibles con los datos en la nube, por medio de aplicaciones en manos de los ciudadanos.

Cada región del mundo experimenta una rápida urbanización. Hoy en día más de la mitad de la población mundial vive en áreas urbanas, y para el 2050 ese número crecerá a cerca del 70 por ciento, o más de 6.000 millones de personas.[1] Aunque algunas áreas experimentarán una mayor urbanización que otras (por ejemplo: India prácticamente duplicará su población urbana entre 2011 y 2031[2]), el dramático crecimiento urbano se ha vuelto un fenómeno verdaderamente global.

Como dirigente de ciudad, gestionar esta extraordinaria tasa de crecimiento puede ser difícil. Los recursos de las ciudades son escasos, el planeamiento se dificulta por las realidades económicas, y los desafíos críticos de la actualidad, como infraestructuras envejecidas, requieren considerable atención. Amplificando los desafíos de una rápida urbanización está la Internet de las Cosas, un término que define una red de gente, dispositivos y sistemas interconectados. Para el 2020 se espera que haya más de 50.000 millones de objetos conectados a Internet.[3] Además, un reciente estudio conducido por Microsoft[4] predice que habrá 4.700 millones de usuarios de Internet en 2025, y cerca de la mitad estará en línea entre 2012 y 2025–casi enteramente de economías emergentes. Muchas de esas conexiones vendrán de dispositivos de banda ancha móvil, como teléfonos y tabletas. Sin embargo, con el incremento de la conectividad se incrementa también el riesgo para los datos, sistemas e infraestructura de la ciudad.

Resiliencia

La resiliencia se ha vuelto importante para las ciudades a la vez que los desafíos físicos, sociales y económicos del siglo XXI se manifiestan en ambientes urbanos.

Por cierto, a medida que las ciudades están más interconectadas, la seguridad cibernética juega un papel crucial en los esfuerzos de resiliencia.

El ambiente cibernético actual plantea riesgos significativos a una ciudad si no son gestionados con determinación. Los siguientes factores juegan un papel en el mejoramiento de la resiliencia:

Mayor acceso a internet para la ciudadanía: El incremento de la conectividad a Internet sostiene la resiliencia de la ciudad proveyendo vías de comunicación, acrecentando la educación y estimulando el crecimiento económico. De acuerdo a la Unión Internacional de Telecomunicaciones (UTI), el 78 por ciento de los hogares de países desarrollados cuenta con acceso a Internet, y la penetración de la banda ancha móvil es del 84 por ciento. Los países desarrollados verán el mayor crecimiento móvil en el 2014, con un 55 por ciento de las suscripciones totales de banda ancha móvil.[5]

Uso de tecnología inteligente. Las ciudades han sido exitosas en el uso de tecnología inteligente, tales como el análisis de grandes bases de datos y aplicaciones móviles, para mejorar los servicios al ciudadano. Durante las Olimpíadas de Verano de 2012 la ciudad de Londres mejoró su sistema de transporte al poner más información a disponibilidad del público. Información sobre interrupciones del servicio y horarios de llegada de autobuses en tiempo real se ofrecían por medio de aplicaciones para teléfonos inteligentes, permitiendo al público recorrer la ciudad en forma segura y eficiente.

Recopilar y compartir información. Recopilar información y compartirla propicia el incremento de la innovación y reduce las amenazas de seguridad. La creación de una consola de seguridad cibernética como la desarrollada por Swan Island Networks,[6] compañía asociada a Microsoft, es una forma en que la información sobre amenazas informáticas puede ser recopilada y compartida. Esta consola configurable consolida cientos de fuentes de datos para proveer a las ciudades una imagen en tiempo real de amenazas presentes, junto con alertas que hacen procesable la información.

1 World Urbanization Prospects: The 2014 Revision. United Nations, Department of Economic and Social Affairs, Population Division. 2014
2 Building and managing intelligent cities in India. Accenture. 17 de Diciembre de 2013. http://timesofindia.indiatimes. com/tech/tech-news/software-services/Proud-that-Indias-a-source-of-global-tech-talent-Satya-Nadella/ articleshow/31750255.cms
3 Evans, Dave. "The Internet of Things: How the Next Evolution of the Internet is Changing Everything." Cisco. Abril de 2011. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
4 Burt, David, Aaron Kleiner, J. Paul Nicholas, y Kevin Sullivan. Microsoft Cyberspace 2025. Microsoft. Junio de 2014. http://download.microsoft.com/download/C/7/7/C7775937-748E-4E95-85FB-24581F16B588/Cyberspace%20 2025%20Today's%20Decisions,%20Tomorrow's%20Terrain.pdf
5 "ITU releases 2014 ICT figures." ITU. 5 de Mayo de 2014. http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#. U4feMKxOXbg
6 "TIES for Microsoft CityNext: Cyber Edition." Swan Island Networks. http://swanisland.net/products/city/cyber-edition

Principios de una estrategia de seguridad cibernética

Una estrategia de seguridad cibernética debería tener una serie de principios claros que propicien un marco de decisión en la identificación, gestión y mitigación de riesgos de seguridad, en forma tal que exista equilibrio entre los derechos civiles, el derecho a la intimidad, costos y otras prioridades en la puja actual hacia ciudades conectadas con la nube y la tecnología móvil. Microsoft recomienda estos principios-guía hacia una estrategia de seguridad cibernética ciudadana:

Principios de seguridad cibernética	**Basada en el riesgo.** Evaluar riesgos identificando amenazas, vulnerabilidades y consecuencias, y gestionarlos por medio de atenuaciones, controles, costos y otras medidas.
	Orientada a resultados. Centrarse en el estado final deseado en lugar de prescribir los medios para lograrlo, y medir el progreso hacia ese estado final.
	Establecer prioridades. Adoptar un enfoque gradual hacia las prioridades, reconociendo que interrupciones y fallas no son iguales entre los activos críticos o a través de sectores críticos.
	Factibilidad. Debe optimizarse para su adopción por el mayor número posible de activos críticos y para su implementación en el mayor rango posible de sectores críticos.
	Respeto a la intimidad y los derechos civiles. Debe incluir protecciones basadas en los Principios de Mejores Prácticas en lo referente a la Información (FIPPs) y otras políticas, prácticas y encuadres sobre privacidad y libertades civiles aceptadas internacionalmente.
	Influencia a escala nacional y global. Debe integrar los estándares nacionales e internacionales de forma lo más extendida posible, con la armonía en mente.

¿Qué es seguridad cibernética?

Para una ciudad, la seguridad cibernética es la protección de datos, sistemas e infraestructura vital para la operatividad y estabilidad de la ciudad y la subsistencia de sus habitantes.

Comprendiendo el panorama de amenazas en el ciberespacio

Antes de desarrollar una estrategia de seguridad cibernética, una ciudad debería examinar su panorama de amenazas. El tipo de amenazas en línea que enfrentan los datos, sistemas e infraestructura de la ciudad han crecido en complejidad e incluyen de todo, desde software malicioso y spam hasta fraude en línea y actividades terroristas.

Datos. El flujo de información es crítico para una ciudad en lo que atañe a su capacidad de mantener los servicios y conectarse con sus ciudadanos. Registros de salud, informes policiales e impuestos comerciales, todo contiene datos que deben ser protegidos. Aunque el uso inteligente de los datos es vital para mejorar los servicios públicos, también implica un incremento de información de identificación personal (PII) en riesgo.

Las amenazas a los datos provienen primariamente de personas, aunque la pérdida de datos debido a desastres naturales (como inundación, tsunami o huracán) puede ocurrir. Algunas amenazas pueden no ser maliciosas, como la descarga involuntaria de software infectado. Por ejemplo, cuando un técnico insertó inadvertidamente una memoria USB infectada en una red de computadoras, el resultado del ataque del virus hizo caer el sistema de control de una turbina de una compañía eléctrica estadounidense durante tres semanas.[7]

7 Finkle, Jim. "Malicious virus shuttered power plant: DHS." Reuters. 16 de Enero de 2013. http://www.reuters.com/ article/2013/01/16/us-cybersecurity-powerplants-idUSBRE90F1F720130116

Amenazas En Línea

Los hackers y otros criminales están acelerando sus ataques a computadoras en todo el mundo, con:

- Software malicioso y spam.
- Tácticas de "phishing".
- Estafas y fraudes en línea.
- Ataques de Denegación de Servicio (DDoS).
- Botnets.
- Piratería de software, infracciones de derechos de autor y violaciones de marcas registradas.

Sin embargo, las amenazas suelen ser maliciosas, como el robo de información privilegiada o la corrupción de datos, o un hacker que instala un botnet o interrumpe servicios con un ataque DDoS. Dos incidentes recientes ilustran las vulnerabilidades de los datos municipales. A finales del 2013, una memoria flash fue robada de un contratista de Milwaukee en los Estados Unidos. La memoria contenía los números de Seguro Social e información personal sin codificar de 6.000 empleados municipales.[8] Además, la ciudad de Johannesburgo, Sudáfrica, sufrió la violación de sus sistemas IT, exponiendo las tasas de clientes y facturas de servicios a potenciales fraudes.[9]

Sistemas. Los sistemas digitales de una ciudad son vitales para la continuidad de sus operaciones. Los sistemas escolares utilizan herramientas en línea para agilizar el aprendizaje y para registrar y realizar el seguimiento del desempeño de los estudiantes. Los sistemas para el cumplimiento de la ley ayudan a la seguridad y protección de los ciudadanos. Los sistemas de comunicación de emergencias son cruciales durante tormentas o emergencias médicas. Si cualquiera de ellos fuera comprometido y causara una interrupción del servicio, los ciudadanos estarían en riesgo. Como con las amenazas a los datos, los sistemas pueden ser comprometidos por acciones tanto maliciosas como involuntarias.

Infraestructura. Muchas grandes ciudades son dueñas, operan o regulan su infraestructura crítica, como la red de distribución eléctrica, la provisión de agua, el transporte. Cada vez más estos servicios públicos clave están siendo sustituidos por sistemas basados en las TIC para mejorar su eficiencia, pero el incremento de la conectividad y la cada vez más extendida tercerización eleva la vulnerabilidad de las infraestructuras a los ataques informáticos. El Departamento de Seguridad Interior de los Estados Unidos ha dicho que el Equipo de Respuesta a Emergencias de Sistemas de Control Industrial respondió a 198 incidentes reportados por compañías eléctricas, de aguas y otras instalaciones de infraestructura en el año fiscal finalizado el 30 de Septiembre de 2012.[10] El tifón Haiyan, en el sudeste asiático, causó una enorme devastación de infraestructura –los sistemas de provisión eléctrica y de comunicaciones quedaron inutilizados, en algunas áreas, durante meses. Adicionalmente, algunos expertos culpan a los ataques informáticos por el apagón del 2003, el mayor apagón de la historia norteamericana, que afectó a 50 millones de personas en un área de 9.300 millas cuadradas, y por el apagón masivo de Florida en 2008, que desconectó grandes porciones de la red eléctrica.[11]

Aprender de Tallinn, Estonia

En la primavera del 2007, redes y sistemas de computación en Estonia fueron objeto de una ataque DDoS masivo originado en el extranjero. Servicios gubernamentales, como la red de correo electrónico del Ministerio de Defensa, además de servicios privados como sitios web de bancos y redes de cajeros automáticos quedaron fuera de servicio, incapacitando efectivamente a la mayoría de las empresas públicas y privadas durante las aproximadamente 48 horas que duró el ataque. No hubo daños físicos. Sin embargo, el ataque paralizó intermitentemente las actividades financieras y gubernamentales del país durante semanas.

El gobierno Estonio y el sector privado aprendieron del incidente cómo proteger mejor sus operaciones. Como resultado, Estonia tiene firmas electrónicas fortificadas, cortafuegos y sistemas de respaldo, y se ha convertido en un campeón de la seguridad cibernética.

8 "Notice of Privacy Incident." United/Dynacare, LLC. 2013. https://www.dynacaremilwaukee.com/Downloads/Dynacare%20SubNotice%20Rev112013.pdf

9 "Breach of Our IT System." City of Johannesburg. 22 de Agosto de 2013. http://www.joburg.org.za/index. php?option=com_content&id=8771:22-08-2013-breach-of-our-it-system

10 "ICS-CERT Monitor." U.S. Department of Homeland Security. https://ics-cert.us-cert.gov/sites/default/files/ICS- CERT_Monitor_April-June2013.pdf

11 Harris, Shane. "China's Cyber-Militia." National Journal. 31 de mayo de 2008. www.nationaljournal.com/magazine/china- s-cyber-militia-20080531

Sentando las bases para desarrollar una estrategia de seguridad cibernética

Otro paso importante que una ciudad debe dar antes de comenzar una estrategia de seguridad cibernética es investigar los requerimientos nacionales y regionales en cuanto a seguridad cibernética. Además, las ciudades deberían examinar el estado de preparación de sus organizaciones internas y entonces abordar el tema del financiamiento de sus estrategias.

Normas y requisitos de investigación

Actualmente, la mayoría de los gobiernos proveen sólo una orientación voluntaria en lo relacionado a seguridad cibernética, pero algunos están comenzando a exigir el cumplimiento de normas, particularmente en lo que se refiere a infraestructuras críticas. Las ciudades deberían, por consiguiente, observar estos desarrollos de cerca. En Japón, un nuevo proyecto de ley requeriría que todos los ministerios y agencias de gobierno informen los ataques informáticos, dando al primer ministro la autoridad para ordenarles obedecer.[12] Similares requerimientos legislativos están siendo contemplados por los dueños y operadores de infraestructuras críticas en otros lugares del mundo, como la Unión Europea. En algunos casos, estos requerimientos podrían aplicarse a infraestructuras críticas que pertenezcan a o estén gestionadas por la ciudad.

Evaluar la disposición de la organización y el entorno IT para apoyar una estrategia de seguridad cibernética.

¿Puede la arquitectura de tecnología de la información (IT) de la ciudad ocuparse adecuadamente de la complejidad que surge del desarrollo de una estrategia de seguridad cibernética? ¿Puede esa estrategia estar alineada con las necesidades de la ciudad? ¿Se adecua a los estándares requeridos?

Para facilitar la implementación y comunicación, es útil desarrollar un mapa claro de todas las agencias y departamentos en los que la estrategia de seguridad cibernética impactará. Esto debería incluir un detalle de aquellas agencias y departamentos que ya han desarrollado planes y políticas de seguridad de información propias y cuán a menudo prueban o ejecutan esos planes.

Además, revisar los resultados de auditorías de seguridad puede ayudar a la ciudad a tener un mejor entendimiento de la eficiencia y eficacia de la gestión, los controles de seguridad técnica y operacional que se necesitan para implementar la estrategia de seguridad cibernética.

12 Mie, Ayako. "New cybersecurity bill would order all ministries to report attacks." Japan Times. 7 de mayo de 2014. www.japantimes.co.jp/news/2014/05/07/national/new-cybersecurity-bill-require-ministries-report-attacks/#.U4fDqqxOXbgimpact-cybercrime2.pdf

Garantizar la financiación

El costo aproximado para la economía global del crimen informático fue

$400.000 millones anuales.

Para la mayoría de las ciudades, equilibrar la seguridad cibernética con otras prioridades presupuestaras puede ser todo un desafío, aunque puede ser atenuado entendiendo cuál es el retorno de la inversión en medidas de seguridad cibernética. En 2014, el Centro de Estudios Estratégicos e Internacionales produjo Pérdidas Netas: Estimación del Costo del Crimen Informático; Impacto Económico del Crimen Informático II, el cual estimaba que el costo aproximado para la economía global del crimen informático fue de $ 400.000 millones anuales –o el 0.8 por ciento del PBI global.[13] Para evaluar el retorno de la inversión en medidas de seguridad cibernética, una ciudad debería considerar el impacto económico de un ataque informático en sus ciudadanos, en la aplicación de la ley, en el empresariado local y en la administración de la ciudad.

Los dirigentes de la ciudad necesitan hacer de la seguridad cibernética una prioridad, y luego buscar eficiencia operativa. Algunas ciudades crean adalides, líderes del gobierno local que impulsan leyes y otras formas de conseguir financiación. La educación también puede jugar un papel importante en la persuasión de las autoridades financieras de la ciudad sobre cuán crítica es la necesidad de seguridad cibernética y cómo encaja en la estrategia general de seguridad de la ciudad. O puede haber un sistema nacional de subsidios para áreas urbanas de alta densidad o alto riesgo.

Incluso sin un gran presupuesto para seguridad cibernética, las ciudades pueden crear un proceso de revisión del presupuesto general de IT que retire sistemas obsoletos y asegure que el proceso de adquisición de nuevos productos y servicios tenga en cuenta un mayor nivel de riesgos de seguridad. El proceso debería también reducir los costos administrativos, crear flexibilidad e incrementar la seguridad.

13 Net Losses: Estimating the Cost of Cybercrime; Economic impact of cybercrime II. Center for Strategic and International Studies. Junio de 2014. www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Crear una estrategia para seguridad cibernética ciudadana

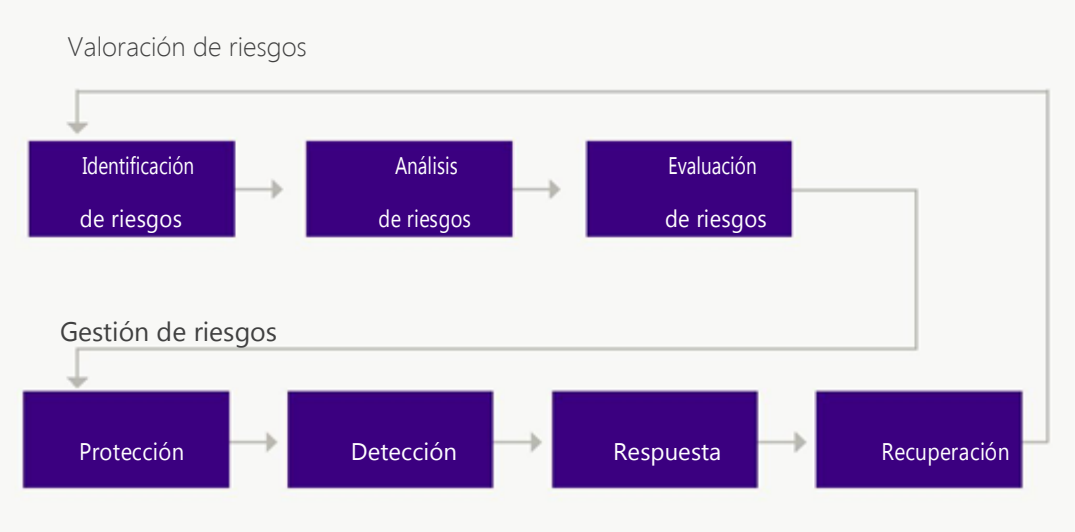
1 Construir un enfoque a la seguridad cibernética basado en los riesgos

El primer paso en el desarrollo de una estrategia de seguridad cibernética se enfoca en la identificación, análisis y evaluación de riesgos a gestionar. Los riesgos en el ciberespacio son típicamente pensados como riesgos para los sistemas de información que, en caso de explotar, podrían impactar negativamente en el bienestar económico de la ciudad o en la seguridad pública de sus ciudadanos en grado significativo.

Un enfoque basado en los riesgos debe contemplar la estructura general de sistemas de la ciudad para determinar dónde se producen las dependencias críticas y averiguar cómo mitigar las vulnerabilidades para reducir la probabilidad de fallas del sistema. Los líderes de la ciudad deberían también considerar llevar a cabo simulaciones y revisiones técnicas para entender las interdependencias y los puntos débiles.

Recomendaciones

→ **Desarrollar una estructura clara para evaluar y gestionar riesgos.** Es recomendable el uso de la siguiente taxonomía:



→**Valorar las amenazas a la seguridad cibernética de la ciudad usando modelización de amenazas.** La modelización de amenazas puede ayudar a identificar los activos que la ciudad trata de proteger, además de aquello de lo cual quiere protegerlos. Un modelo de amenazas realiza un inventario de activos municipales clave y sus amenazas, determina la probabilidad de que esos activos necesiten protección, observa la capacidad de la ciudad para defenderse contra las amenazas y determina las consecuencias de la inacción. Este enfoque permite a los líderes de la ciudad identificar y mitigar potenciales problemas de seguridad tempranamente, mientras los problemas son relativamente fáciles y económicos de resolver. Categorizar las amenazas en línea (como se muestra en la tabla siguiente) puede facilitar la valoración de amenazas para luego desarrollar estrategias preventivas y reactivas específicas.

Amenaza		Ejemplos
Pasivas	Acciones involuntarias	Exposición a malware por email o sitios web Recepción de correo spam o phishing
	Recursos insuficientes	Sistemas desprotegidos Estrategias de mitigación poco claras Capacidad de respuesta indefinida Pertenencia poco clara
Activas	Crimen cibernético	Fraude Ataques de denegación de servicio Robo de propiedad intelectual o financiera Abuso o daño a sistemas TIC Daños a infraestructura crítica
	Peligros naturales	Tifones y huracanes Terremotos y tsunamis Inundaciones Tsunamis Corte accidental de cableado submarino de Internet

→ **Documentar y revisar la aceptación de riesgos y excepciones.** Al implementar una estrategia de seguridad cibernética basada en los riesgos, los líderes de la ciudad encuentran a menudo que para que el gobierno pueda brindar servicios, simplemente deben aceptarse algunos riesgos. Es imposible mitigar todos los riesgos, y un encuadre de riesgos debería incluir directivas claras que rijan tanto para los riesgos aceptables como para aquellos casos en que los activos son tan vitales que deben ser protegidos. El riesgo aceptable y cualquier excepción relevante debería ser aprobada por la dirección de la agencia responsable; En algunas instancias, esos riesgos deberían ser sometidos a las máximas autoridades de la ciudad para su aprobación.
Dentro de la estrategia de seguridad cibernética, los líderes de la ciudad deberían asignar responsabilidades por los riesgos aceptables al personal pertinente y desarrollar planes de respuesta a incidentes apropiados para la gestión de esos riesgos. Los registros de riesgos aceptables deberían ser revisados regularmente para asegurar que sistemas críticos, ya sean públicos o privados no queden innecesariamente expuestos.

→ **Hacer de la valoración y gestión de riesgos de la ciudad un proceso continuo.** La valoración y gestión de riesgos debería ser un proceso continuo, no un estado final. A medida que la tecnología evoluciona y las amenazas crecen en sofisticación, debe haber evaluaciones en curso para valorar si los controles siguen siendo adecuados. Además, puede aparecer tecnología que permita una efectiva mitigación de riesgos que previamente fueron considerados aceptables.

Más información sobre la construcción de un enfoque de seguridad cibernética basado en los riesgos:

- Local Government Cyber Security: Risk Management, A Non-Technical Guide: http://msisac.cisecurity.org/members/local-government/documents/Cyber-Security-Risk-Management-for-Local-Governments.pdf
- ISO Standard 31000:2009 Risk management—Principles and guidelines: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
- National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091

2 Establecer prioridades claras

Toda ciudad confía en ciertos servicios y funciones críticas o gestiona información sensible que, si es comprometida, dañada o destruida por un incidente de seguridad cibernética, podría impactar dramáticamente en su capacidad de funcionamiento. El desafío de priorizar qué sistemas proteger implica difíciles disyuntivas.

Aunque es tentador identificar todos los activos municipales como alta prioridad, es crítico tener un proceso claro de priorización. Los líderes de la ciudad deben revisar los principios de la estrategia y alinear las prioridades acorde a ello. Es importante definir e implementar un encuadre claro de clasificación de sistemas y datos como de alto, medio o bajo impacto, para luego usar esto para evaluar los sistemas clave de la ciudad, incluso aquellos operados por terceras partes. Adicionalmente, para asegurar un enfoque común en toda la estructura empresarial de la ciudad, la ciudad debería trazar un mapa de perfiles de protección para la clasificación de sistemas y datos.

Una de las mejores maneras de priorizar riesgos es usar estándares existentes. Sin embargo, a menudo los riesgos evolucionan demasiado rápido para ser incluidos en los organismos oficiales de estandarización. Actividades de gestión de riesgos adicionales, como un enfoque de "los 20 principales controles críticos de seguridad", propugnado por organizaciones como SANS,[14] pueden elevar los estándares para ayudar en la priorización.

En febrero de 2014, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos libró un encuadre voluntario que incluye estándares, directivas y prácticas que pueden ser usados por ciudades para gestionar riesgos relacionados con la seguridad cibernética. Aunque fue publicado en los Estados Unidos, el encuadre se basa en trabajos hechos alrededor de todo el mundo y puede ser aplicado a la mayoría de las ciudades. Otro recurso es "Controles Críticos de Seguridad", que ofrece métodos tangibles para identificar riesgos para los datos y sistemas de empresas.

Recomendaciones

→Educar a los líderes de la ciudad para entender y apoyar los principios y gestionar prioridades. Puede ser difícil sopesar ventajas y desventajas al establecer prioridades. Una educación de rutina de los líderes de la ciudad en los principios de la seguridad cibernética facilita la negociación de prioridades. No todos los líderes tienen experiencia en seguridad cibernética, pero todos pueden incorporarse al proceso de establecer prioridades y de comprender cómo impactan sus decisiones en los activos de la ciudad.

→Considerar la resiliencia. La infraestructura de una ciudad tiene poco valor si no está consistentemente disponible. La estrategia de una ciudad debería priorizar recursos, estándares y soporte organizacional para asegurar que los servicios más esenciales tengan un mayor grado de resiliencia que los servicios menos críticos. Por ejemplo, la migración a un servicio basado en la nube es una forma de proveer ancho de banda adicional y capacidad de asegurar la provisión del servicio durante una crisis.

→Aprovechar los procesos de adquisición para reflejar prioridades y riesgos. Las ciudades deben asegurarse de que sus prioridades estén reflejadas en las adquisiciones de IT. Pueden utilizar el proceso de adquisición para aprender sobre nuevas tecnologías o capacidades que puedan incrementar la seguridad cibernética de la ciudad y refinar el modo en que la ciudad piensa acerca del ciclo de vida de su tecnología.

Más información sobre establecer prioridades de seguridad cibernética

- NIST Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
- SANS Institute Critical Security Controls for Effective CyberDefense: www.sans.org/critical-security-controls

14 "Critical Security Controls for Effective CyberDefense." SANS Institute. www.sans.org/critical-security-controls

3 Definir los lineamientos de seguridad TIC mínimos

Un lineamiento de seguridad mínima es un estándar de seguridad mínimamente aceptable (o mejor práctica) diseñado para asegurar que los departamentos de la ciudad implementen medidas básicas de seguridad para reducir el riesgo de acceso no autorizado a datos y recursos IT. Las prácticas de seguridad pueden incluir protocolos para parches de seguridad, desactivación de servicios innecesarios o estándares de higiene de escritorio.

Recomendaciones

→**Establecer lineamientos de seguridad mínimos.** Al establecer los lineamientos, una ciudad evalúa las prácticas de seguridad TIC existentes de sus departamentos y establece estándares mínimos para la seguridad TIC de los datos, sistemas e infraestructura gubernamental.
Pero un lineamiento es sólo eso –un punto de partida desde el cual los líderes de la ciudad deberían continuar propulsando mejoras de seguridad. A medida que las ciudades mejoran sus procedimientos de seguridad con regularidad, los lineamientos deben ser reevaluados. Hay una cantidad de áreas en las que aplicar los lineamientos, incluyendo la seguridad cibernética de los sistemas propios, los indirectos (tránsito, aguas, educación y salud), proveedores y ciudadanos.

→**Definir funciones y responsabilidades claros para apoyo de los lineamientos de seguridad.** Si no hay una agencia central responsable de la seguridad TIC, la estrategia de seguridad cibernética debería recomendar establecer una agencia con personal idóneo, junto con un nivel de autoridad adecuado y los recursos necesarios para desarrollar los lineamientos de seguridad TIC.

→**Establecer un sistema de monitoreo continuo de seguridad.** En un ambiente donde las amenazas cambian constantemente, la estrategia de seguridad cibernética de una ciudad debería reconocer la necesidad del monitoreo constante de seguridad de los sistemas, datos e infraestructura, en lugar de enfocarse en auditorías y chequeos de observancia realizados en papel. El monitoreo continuo automatiza la recolección y análisis de datos de una variedad de fuentes para mantener una descripción precisa de la postura de seguridad de la organización. Unas capacidades de monitoreo adecuadas pueden ofrecer datos para determinar si se ha comprometido algo, y esas capacidades puede sustentar decisiones de gestión de riesgos.

Hay estándares, como los controles de seguridad y privacidad establecidos por el NIST en su publicación 800-53, que identifica el monitoreo continuo separando los servicios de monitoreo en cuatro categorías:

- Lineamientos de monitoreo de seguridad para detección amplia de actividades de red anómalas o maliciosas.
- Monitoreo de seguridad especializado para activos y procesos críticos.
- Análisis y reporte de datos para proveer telemetría para la detección de seguridad interna clave y socios de respuesta.
- Aplicación de políticas y medición de la eficacia de los controles.

Más información sobre el establecimiento de lineamientos de seguridad TIC

- NIST Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800-53 (revision 4): nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- Council on Cybersecurity's Critical Security Controls for Effective CyberDefense: https://ccsfiles.blob.core.windows.net/web-site/file/c9665df3a5f54d2b8e6edab493c3b076/CSC-MASTER- VER50-2-27-2014.pdf
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Un informe publicado por Verizon encontró que el

97%

de los incidentes de violación de redes investigados durante el 2012 pudieron haber sido prevenidos por medio del uso de controles de seguridad simples o intermedios.[15]

15 Verizon RISK Team. 2012 Data Breach Investigations Report. 22 de marzo de 2012. http://www.verizonenterprise.com/ resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

4 Compartir y coordinar información sobre amenazas y vulnerabilidades

El año pasado, el

50%

de los adultos en línea fueron víctimas de crímenes informáticos. [16]

Las amenazas a y vulnerabilidades de los sistemas TIC son moneda corriente para aquellos que explotan los activos de la ciudad –y para aquellos que pretenden atacar. En un ambiente de amenazas en constante evolución, quienes se ocupan de las respuestas de seguridad necesitan información actualizada al minuto sobre amenazas o vulnerabilidades para proteger estos activos. La información sobre amenazas necesita ser compartida tan rápido como sea posible a la audiencia más vasta posible, para que los perpetradores de la amenaza puedan ser detenidos con el mínimo daño. La estrategia de seguridad cibernética de una ciudad debería desarrollar criterios respecto de dónde y cuándo compartir esta información.

Esto también puede ayudar a encontrar nuevas protecciones o mitigaciones, a veces incluso antes de cualquier impacto negativo. Si se hace con la suficiente amplitud y eficiencia, el intercambio de información de amenazas elimina la ventaja de los ataques tempranos y prevé la explotación de vulnerabilidades en la seguridad, tanto de grupos externos como internos. Una estrategia de seguridad cibernética puede ayudar a construir un modelo colaborativo en el que la información se comparte, y quienes estén mejor posicionados para actuar podrán hacerlo.

Compartir información sobre amenazas es sólo el primer paso. Debe haber pasos adicionales de acción que las agencias de la ciudad y los ciudadanos puedan tomar luego que las vulnerabilidades sean expuestas. El descubrimiento, en abril del 2014, del error de seguridad Heartbleed en OpenSSL, que permitió el robo de claves privadas de aproximadamente medio millón de servidores web seguros y que hizo que las session cookies y claves fueran vulnerables a los hackers,[17] arroja luz sobre cómo y cuándo los gobiernos comparten información.

Recomendaciones

- **Establecer expectativas sobre el intercambio de información sobre amenazas y vulnerabilidades.** Todos se benefician cuando la ciudad se asocia a entidades nacionales y el sector privado para compartir rápidamente información sobre nuevas amenazas y vulnerabilidades. La estrategia de seguridad informática de una ciudad debería recomendar una vía de comunicación clara entre la ciudad, la región, el gobierno federal y el sector privado.

- **Crear un mecanismo de intercambio para la ciudad.** La estrategia de una ciudad debería incluir mecanismos de intercambio de información sobre incidentes e indicadores de compromiso. Las ciudades deberían compartir su información sobre amenazas con sus agencias para una mejor gestión de riesgos y para alentar la cooperación y el aprendizaje entre los profesionales TIC de la ciudad. Además, las ciudades pueden querer compartir información con los dueños de infraestructura e industria crítica, y con compañías que tengan la capacidad de desarrollar y distribuir actualizaciones a sus clientes. Contar con el correcto marco legal y técnico para propiciar el intercambio ayuda a asegurar un proceso de respuesta más efectivo, y ayuda también a las partes a enfocarse en las amenazas esenciales. Este intercambio de información abierto promueve unas alianzas más fuertes con el sector privado y propicia que todos estén enfocados en las amenazas más críticas.

- **Probar los planes de juego con "cibertaladros".** Taladrar con escenarios reales debería incluir a todos los miembros del equipo de respuesta a incidentes en línea de una ciudad –personal de la ciudad, del estado y agencias federales, además de participantes del sector privado. Las ciudades pueden proveer recursos para ayudar a las empresas locales correr sus propios taladros, como aquellos que corrieran en la ciudad de San Diego en alianza con la Escuela Naval de Posgrado. [18]

16 Warnick, Jennifer. "Microsoft, Digital Detectives." 2014. http://www.microsoft.com/en-us/news/stories/ cybercrime/index.html
17 "The Heartbleed Bug." Codenomicon. http://heartbleed.com/
18 Dodd, David. "Channel Your Inner Hacker and Other Cyber Security Suggestions." Forbes. October 11, 2013. www.forbes.com/sites/xerox/2013/10/11/channel-your-inner-hacker-and-other-cyber-security- suggestions/

→ **Enfatizar la protección de la privacidad y las libertades civiles en el intercambio de información de amenazas.** Ha habido muchas discusiones sobre el nivel apropiado de información que debería compartirse entre entidades del sector privado que responden a vulnerabilidades o amenazas y entre aquellas entidades del sector privado y agencias municipales. Es importante que la estrategia de la ciudad enfatice eso, independientemente del escenario o tipo de dato compartido, los pasos están en su lugar para asegurar que la privacidad siempre sea tenida en cuenta. Además, asegurar una adecuada supervisión y aplicación judicial de la protección de la privacidad es esencial. Las prácticas que rigen el intercambio de información sobre amenazas y vulnerabilidades deben también acatar las leyes de privacidad existentes en la ciudad y el país, e incluso internacionalmente, puesto que la información podría compartirse fronteras afuera.

→ **Aplicar los estándares de intercambio de información nacionales o internacionales relevantes.** Los conceptos de fomentar enfoques comunes de valoración y gestión de amenazas y vulnerabilidades y de intercambio de información sobre ellas deberían estar incorporado en la estrategia de seguridad cibernética de una ciudad.

Por ejemplo, las ciudades pueden utilizar los estándares ISO/Comisión Electrotécnica Internacional (ISO/IEC) en el manejo de vulnerabilidades dentro de una empresa (ISO/IEC 30111) y en divulgación de vulnerabilidad externa a la empresa (ISO/IEC 29147). Estos estándares mejoran en gran medida la capacidad de manejar asuntos complicados relacionados con la respuesta. También fomentar un mayor uso de los identificadores de Vulnerabilidades y Desprotecciones, y dar pasos para evaluar la severidad y explotabilidad de una vulnerabilidad puede incrementar la capacidad y disponibilidad para eventos de respuesta compleja. También existen estándares de intercambio de información entre máquinas, como el Structured Threat Information eXpression (STIX) y el Trusted Automated eXchange of Indicator Information (TAXII) para representar información estructurada de amenazas.

Más información sobre intercambio y coordinación de información sobre amenazas y vulnerabilidades

- ISO/IEC 30111:2013: Information technology—Security techniques—Vulnerability handling processes: https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-1:v1
- ISO/IEC 29147:2014: Information technology—Security techniques—Vulnerability disclosure: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail. htm?csnumber=45170
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

5 Construir capacidad de respuesta a incidentes

Centro de Comando de Ciberintrusión de Los Angeles

Operado por el Departamento de Policía de Los Angeles, integrado por gente de la ciudad y de agencias federales, este centro de operaciones que trabaja las 24 horas monitorea en línea las amenazas contra la ciudad, y sus miembros se reúnen con regularidad para discutir amenazas comunes y posibles métodos para neutralizarlas.

La respuesta a amenazas en línea requiere capacidades suficientes para proteger a la gente, la información, los sistemas y la infraestructura de una ciudad. La estrategia de seguridad cibernética de una ciudad debería, por lo tanto, delinear claramente qué constituye un incidente que requiera que la ciudad se involucre y dispare planes y procedimientos de respuesta a incidentes, y qué constituye uno que sea responsabilidad del sector privado, con un plan de comunicaciones que sirva de puente entre ambos.

Como se indicó antes, las amenazas deberían ser priorizadas y debería desarrollarse una jerarquización de amenazas y respuestas asociadas, estructurada en base a los efectos esperados. Para las ciudades es importante reconocer que una amenaza a sistemas de infraestructura crítica, como el agua, o la energía, requiere respuestas significativamente diferentes que aquellas que afectan a un grupo de sistemas o datos aislados.

Integrar la respuesta a incidentes en una estructura de comando de incidentes existente es otro elemento crítico de la estrategia. En la mayoría de las ciudades, la aplicación de la ley y los servicios de emergencia pueden proveer recursos establecidos y personal para una respuesta en línea. El departamento de policía de una ciudad puede incluir un equipo de informática forense que ayude a identificar, contener y frustrar amenazas en línea.

Los centros de fusión, centros de intercambio de información desarrollados originalmente en los primeros años de la década del 2000 bajo el Departamento de Seguridad Nacional de los Estados Unidos ofrece un buen modelo de integración de la capacidad de respuesta a incidentes existente con la seguridad cibernética. Estos centros potencian la primera línea de aplicación de la ley, seguridad pública, servicio de bomberos, respuesta a emergencias, salud pública, protección de infraestructura crítica y personal de seguridad del sector privado para recolectar, analizar y compartir información relacionada con amenazas.

Recomendaciones

- **Crear un Equipo de Respuesta a Emergencias Computacionales (CERT).** Los gobiernos locales, empresas privadas y universidades puede trabajar juntos para desarrollar CERTs que coordinen la respuesta a incidentes de seguridad computacional. Para ayudar a constituir un CERT municipal, el Foro Global de Respuesta a Incidentes y Equipos de Seguridad es un excelente recurso. [19]
- **Crear una clara identificación.** La estrategia de seguridad cibernética debería recomendar que el CERT lidere cualquier coordinación entre sectores públicos y privados que respondan a incidentes de seguridad en línea. La estrategia debería encargar al CERT las tareas técnicas y de gestión para que asista con efectividad al gobierno y a los actores privados críticos durante situaciones de crisis.
- **Conectarse con el sector privado y los recursos nacionales.** Las agencias municipales deberían trabajar con el sector privado para responder a incidentes en línea. Esto incluye claras vías de comunicación para el intercambio de información sobre amenazas y vulnerabilidades, recursos y entrenamiento. Por ejemplo, la Policía de la ciudad de Londres desarrolló un programa con la Asociación de Banqueros Británicos para entrenar a miles de empleados bancarios cada año en la identificación y respuesta a crímenes informáticos y fraudes en el sector financiero. El programa planea preparar talleres sobre identificación y mitigación de amenazas para bancos de todo el mundo
- **Facilitar una clasificación consistente de incidentes. .** Al diseñar las respuestas a incidentes, las ciudades deben distinguir claramente entre aquellos incidentes que requieren una respuesta de la ciudad y aquellos que no alcanzan a llegar a ese nivel. Debido a que los sistemas e informaciones críticas en manos de privados son posibles blancos de ataques informáticos, la ciudad debe asegurarse que dichos operadores tengan una clara comprensión del papel del gobierno, incluyendo la aplicación de la ley, en caso de un ataque. El papel de la ciudad, ya sea proveyendo defensa directa o apoyo indirecto, varía de acuerdo a las relaciones entre proveedores privados de infraestructura crítica y el gobierno.

19 FIRST. http://www.first.org/

→ **Probar capacidades y procesos de respuesta a incidentes.** De la misma forma que las ciudades prueban su capacidad de manejo de catástrofes importantes, como huracanes y actividades terroristas, deberían planear pruebas para aquellos procesos creados para comunicar, colaborar y restablecer servicios en caso de un incidente informático. Las capacidades de respuesta deberían también ser evaluadas rutinariamente contra el escenario de amenazas informáticas actual.
Al integrarlos con los procedimientos de respuesta existentes a cargo de los departamentos de bomberos y policía, estos esfuerzos se vuelven más efectivos y son mejor gestionados y escalados. Una estrategia de seguridad cibernética debería incluir expectativas específicas para el sector privado y para otras entidades gubernamentales. Ejercicios que involucren tanto a los actores municipales como del sector privado ayuda a los interesados a entender su papel durante una crisis y puede prepararlos mejor para responder a incidentes.

Más información sobre construir capacidad de respuesta a incidentes

- Forum of Incident Response and Security Teams: www.first.org
- NIST Computer Security Incident Handling Guide: http://csrc.nist.gov/publications/ nistpubs/800-61rev2/SP800-61rev2.pdf

6 Fomento de la concientización pública, educación y entrenamiento de la fuerza laboral

Un gran número de incidentes de seguridad en línea son causados por acciones involuntarias de empleados o ciudadanos. Sólo se necesita que una persona cliquee un enlace infectado, abra un correo de origen supuestamente confiable o inserte una memoria USB infectada en una computadora para poner en riesgo información o una red de sistemas completa. Las ciudades pueden ofrecer a sus empleados y ciudadanos herramientas y mejores prácticas no sólo para ayudarlos a proteger los activos municipales, sino también ahorrar dinero en prosecución de crímenes informáticos y limpieza. Entrenamiento y educación deberían ocupar un lugar central en el enfoque para mejorar la seguridad cibernética.

Pasos simples para protección informática

- Instalar software antivirus y actualizarlo con regularidad.
- Instalar hardware/software como un cortafuego para gestionar comunicaciones entre redes y dentro de ellas.
- Tener copias de respaldo de archivos importantes en la nube o en otro lugar.
- Obligar a los usuarios autenticarse al firmar.
- Instalar regularmente parches de sistema operativo.
- Proteger dispositivos móviles con PINs, y mantener al día sus sistemas operativos y aplicaciones.

Recomendaciones

→ **Desarrollar campañas de concientización pública.** La estrategia debería incluir la existencia de una agencia o entidad dedicada a concientizar al público sobre los riesgos en línea y la necesidad de seguridad cibernética. La ciudad de Boston patrocina una campaña de este tipo, que eleva la conciencia pública sobre seguridad cibernética, alentando a los ciudadanos a tomar un compromiso informático que incluye educación sobre navegación segura y medidas de seguridad en dispositivos, junto con advertencias sobre cuándo y dónde es seguro compartir información personal en línea. Ya en 1999 la Comisión Europea lanzó el Programa de Internet Segura, que derivó en el Día de la Seguridad en Internet, un evento anual que destaca la importancia de la seguridad y protección en línea, actualmente se desarrolla en 100 países.

Los distritos escolares pueden jugar un papel importante educando a los jóvenes en seguridad y comportamiento inteligente en línea. StaySafeOnline.org desglosa la seguridad cibernética en pasos sencillos y provee lecciones, actividades y ejercicios para todos los niveles.

Algunos ciudadanos de más edad pueden ser más vulnerables a las amenazas en línea porque tienen menos experiencia en el uso de Internet. Las ventanas emergentes (pop-up) pueden confundir a los mayores y llevarlos a descargar software infectado, y las estafas de correo electrónico de phishing pueden seducirlos a entregar información personal y financiera a criminales. Las ciudades pueden trabajar con organizaciones dedicadas a los mayores en la divulgación de formas de estar a salvo en el ciberespacio. Una alianza público-privada muy útil es el programa eSeniors, desarrollado entre la ciudad de Miami y Microsoft, que provee entrenamiento informático gratuito y descuentos en tecnología a los mayores en Centros Vecinales para la Tercera Edad de Miami. [20]

→ **Propiciar el desarrollo de empleados y programas de entrenamiento de la fuerza laboral.** A menudo las ciudades tienen dificultades para atraer y retener una fuerza laboral talentosa porque no pueden ofrecer salarios y beneficios comparables a los de las empresas privadas. Incentivos como descuentos en matrículas universitarias y entrenamiento especializado pueden ayudar a cerrar esa brecha.

Más información sobre educación y entrenamiento en seguridad cibernética

- Multi-State Information Sharing and Analysis Center (MS-ISAC) Local Government Cyber and Information Security Policies: msisac.cisecurity.org/resources/local-cyber-policies.cfm
- Stay Safe Online: www.staysafeonline.org
- InSafe's Safer Internet Day: www.saferinternet.org

20 "Microsoft, Miami Offer Seniors Free Computer Training, Customized PCs." 29 de octubre de 2007. www.microsoft.com/en-us/news/press/2007/oct07/10-29eseniorspr.aspx

7 Facilitar la cooperación pública, privada y académica

La colaboración con el sector privado, otras entidades del sector público e instituciones académicas para investigar, identificar y responder a amenazas en línea debe ser un componente primordial en la estrategia de seguridad cibernética de una ciudad.

En ciudades donde las entidades privadas que gestionan infraestructura crítica son controladas por el gobierno, una estrategia de seguridad cibernética de la ciudad puede formalizar la creación alianzas público-privadas. La "Guía de Mejores Prácticas en Modelos de Cooperación para Alianzas Público-Privadas Efectivas", detallada en la página siguiente, ofrece 36 recomendaciones sobre cómo construir alianzas exitosas para una seguridad resiliente.

En cuanto a la colaboración entre ciudades, las mismas pueden mirar el trabajo del Grupo de Liderazgo Climático C40 como modelo. En el 2005, mega-ciudades de todo el mundo se unieron para reducir las emisiones de carbono y mejorar la eficiencia energética. Liderado por alcaldes y dirigentes de las ciudades, el C40 colabora estrechamente con las ciudades participantes para identificar los riesgos climáticos y su impacto a nivel local y global.

Recomendaciones

- **Aprovechar las ventajas de los recursos del sector privado.** Las empresas locales generalmente participan de la vida cívica con programas que van desde intercambio de ejecutivos a entrenamiento especializado. Una estrategia de seguridad cibernética debería recomendar la creación de programas que incluyan empresas del sector privado, particularmente empresas de tecnología. Un programa de intercambio de ejecutivos en el que empleados del sector privado se desempeñan como empleados municipales ad honorem, puede satisfacer necesidades específicas de seguridad cibernética dentro de la organización TIC de la ciudad, y puede proporcionar conocimientos y nuevas perspectivas. Las ciudades también pueden trabajar con aliados del sector privado para fomentar la aceleración del desarrollo de nuevas empresas de tecnología y fuentes de trabajo. Por ejemplo, Microsoft tiene Centros de Innovación de Tecnología de Avanzada en más de 100 ciudades en todo el mundo, ofreciendo a las organizaciones acceso a recursos, expertos y herramientas valiosas para la colaboración y el desarrollo de habilidades.
- **Alianzas con universidades.** Si no hay una agencia central responsable de la seguridad TIC, la estrategia de seguridad cibernética debería recomendar establecer una agencia con personal idóneo, junto con un nivel de autoridad adecuado y los recursos necesarios para desarrollar los lineamientos de seguridad TIC.
- **Patrocinar eventos de integración entre el sector público y privado.** Dichos eventos pueden ser desde grandes cumbres anuales de participantes internacionales hasta encuentros más pequeños y frecuentes con emprendedores para impulsar el pensamiento creativo.
- **Promover la cooperación en cuanto a aplicación de la ley a la vez que se protegen la privacidad y las libertades civiles.** Las agencias de aplicación de la ley deben contar con formas de trabajar con los organismos de respuesta de todo el mundo, al margen de sus diferencias en cuanto a privacidad y capacidades tecnológicas. Una estrategia de seguridad cibernética debería recomendar que una única entidad, preferentemente dentro del departamento de policía existente, sea responsable de asuntos de seguridad cibernética, y que esté provista de los recursos y entrenamiento adecuados, acompañado de legislación adecuada y supervisión que garantice el respeto y la protección de la privacidad y las libertades civiles.

→ **Crear una cultura de innovación tecnológica.** Una cultura de la innovación impulsa a las organizaciones a prosperar en la nueva economía. Las ciudades pueden crear ambientes que propicien la innovación. Por ejemplo, Tech City UK tiene el objetivo de ayudar a los negocios digitales en Londres a crecer y desarrollar nuevas ideas. Proporciona asesoramiento en todo, desde reclutamiento de personal, preparación de cuentas y conformidad a la negociación de arriendos, mercadeo y aumento de inversión. En febrero de 2014, durante la peor inundación registrada en la historia del Reino Unido, varias agencias gubernamentales brindaron información sobre el nivel de inundación durante todo un día #floodhack, alojado por Tech City UK, permitiendo a los desarrolladores crear soluciones innovadoras para desastres relacionados con el clima.

Más información sobre cooperación pública, privada y académica

- EU Agency for Network and Information Security's Good Practice Guide on Cooperative Models for Effective PPPs: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps
- C40Cities Climate Leadership Group: www.c40.org
- Microsoft Innovation Centers: www.microsoftinnovationcenters.com
- Tech City UK: www.techcityuk.com

Conclusión

Establecer una estrategia de seguridad cibernética para la ciudad es un elemento importante para el mantenimiento de la seguridad ciudadana mientras se traza una ruta hacia el futuro. Por medio de la creación de un enfoque estructurado, pensando integralmente sobre amenazas y vulnerabilidades, e implementando prácticas sólidas para detectar, mitigar y comunicar amenazas, una ciudad puede proteger a sus habitantes y salvaguardar sus recursos. Sin embargo habrá obstáculos. Presupuestos acotados pueden limitar el planeamiento y desarrollo. Dirigentes municipales reacios a correr riesgos pueden obstaculizar la colaboración y la innovación. Inquietudes sobre la privacidad pueden limitar las actividades. Por medio de una clara articulación del retorno de la inversión –financiera, de seguridad y de calidad de vida–, una estrategia de seguridad cibernética puede superar estos obstáculos y pasar a formar parte integral de la transformación de la ciudad.

Microsoft apoya los esfuerzos de los municipios para desarrollar estrategias de seguridad cibernética. Con gran parte de la población mundial localizada en áreas urbanas, las ciudades están excepcionalmente posicionadas para confrontar y gestionar temas de seguridad cibernética. Microsoft está dispuesta a ayudar a los líderes de la ciudad a mantener a sus comunidades, y al mundo, seguro y protegido.

Lista de control de estrategia de seguridad cibernética

1. **Construir un enfoque a la seguridad cibernética basado en los riesgos**

- ☐ Desarrollar una estructura clara para evaluación y gestión de riesgos.
- ☐ Evaluar las amenazas a la seguridad cibernética de la ciudad usando modelado de amenazas.
- ☐ Documentar y revisar riesgos aceptables y excepciones.
- ☐ Hacer de la evaluación y gestión de riesgos un proceso continuo.

2. **Establecer prioridades claras**

- ☐ Educar a los líderes de la ciudad para entender y apoyar los principios y gestionar prioridades.
- ☐ Considerar la resiliencia.
- ☐ Aprovechar los procesos de adquisición para reflejar prioridades y riesgos.

3. **Definir los lineamientos de seguridad TIC mínimos**

- ☐ Establecer lineamientos de seguridad mínimos.
- ☐ Definir funciones y responsabilidades claras para apoyo de los lineamientos de seguridad.
- ☐ Establecer un sistema de monitoreo continuo de seguridad.

4. **Compartir y coordinar información sobre amenazas y vulnerabilidades**

- ☐ Establecer expectativas sobre el intercambio de información sobre amenazas y vulnerabilidades.
- ☐ Crear un mecanismo de intercambio para la ciudad.
- ☐ Probar los planes de juego con "cibertaladros".
- ☐ Enfatizar la protección de la privacidad y las libertades civiles en el intercambio de información de amenazas.
- ☐ Aplicar los estándares de intercambio de información nacional o internacionales relevantes.

5. **Construir un enfoque a la seguridad cibernética basado en los riesgos**

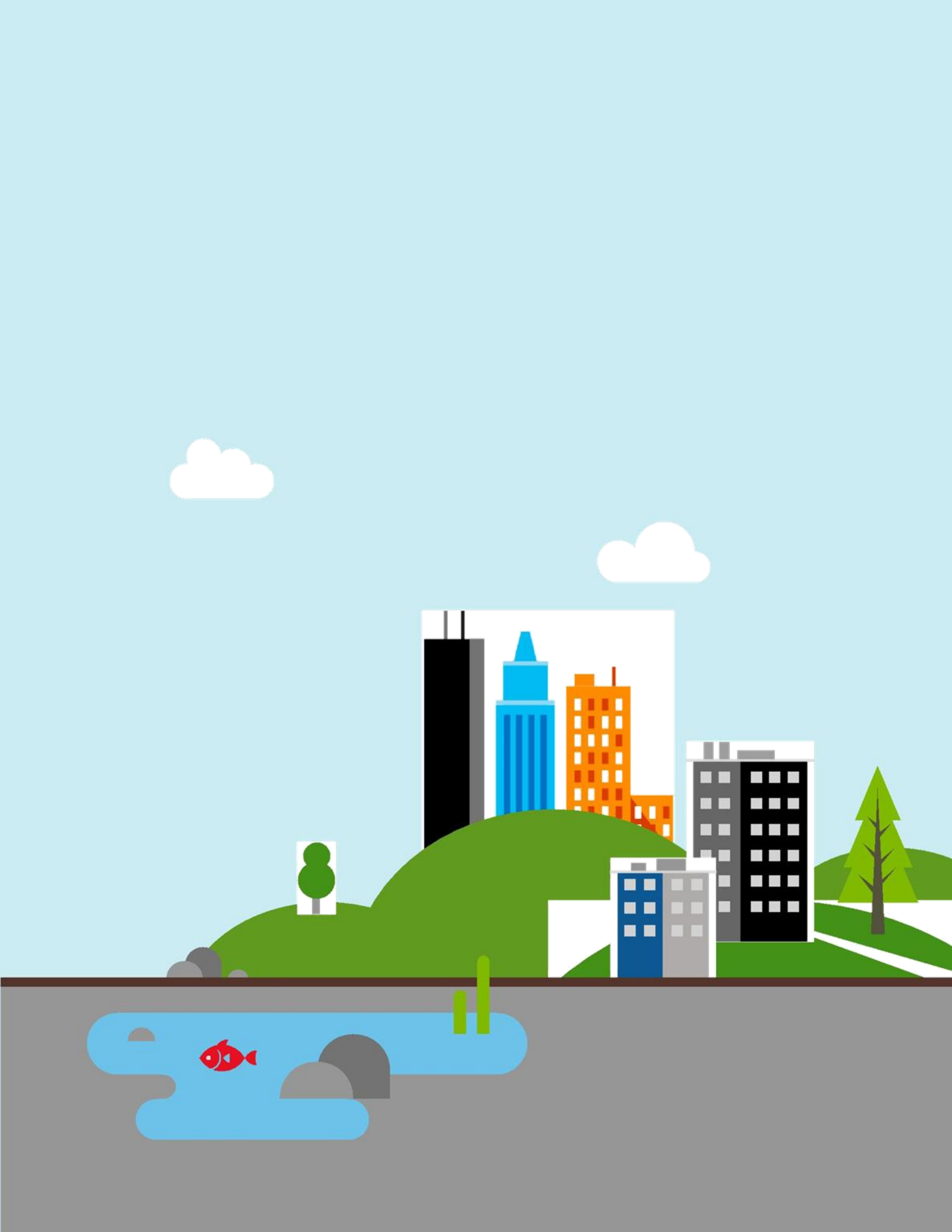
- ☐ Crear un Equipo de Respuesta a Emergencias Computacionales (CERT).
- ☐ Crear una clara identificación.
- ☐ Conectarse con el sector privado y los recursos nacionales.
- ☐ Facilitar una clasificación consistente de incidentes.
- ☐ Probar capacidades y procesos de respuesta a incidentes.

6. **Fomento de la concientización pública, educación y entrenamiento de la fuerza laboral**

- ☐ Desarrollar campañas de concientización pública.
- ☐ Propiciar el desarrollo de empleados y programas de entrenamiento de la fuerza laboral.

7. **Facilitar la cooperación pública, privada y académica**

- ☐ Aprovechar las ventajas de los recursos del sector privado.
- ☐ Alianzas con universidades.
- ☐ Patrocinar eventos de integración entre el sector público y privado.
- ☐ Promover la cooperación en cuanto a aplicación de la ley a la vez que se protegen la privacidad y las libertades civiles.
- ☐ Crear una cultura de innovación tecnológica.



Microsoft