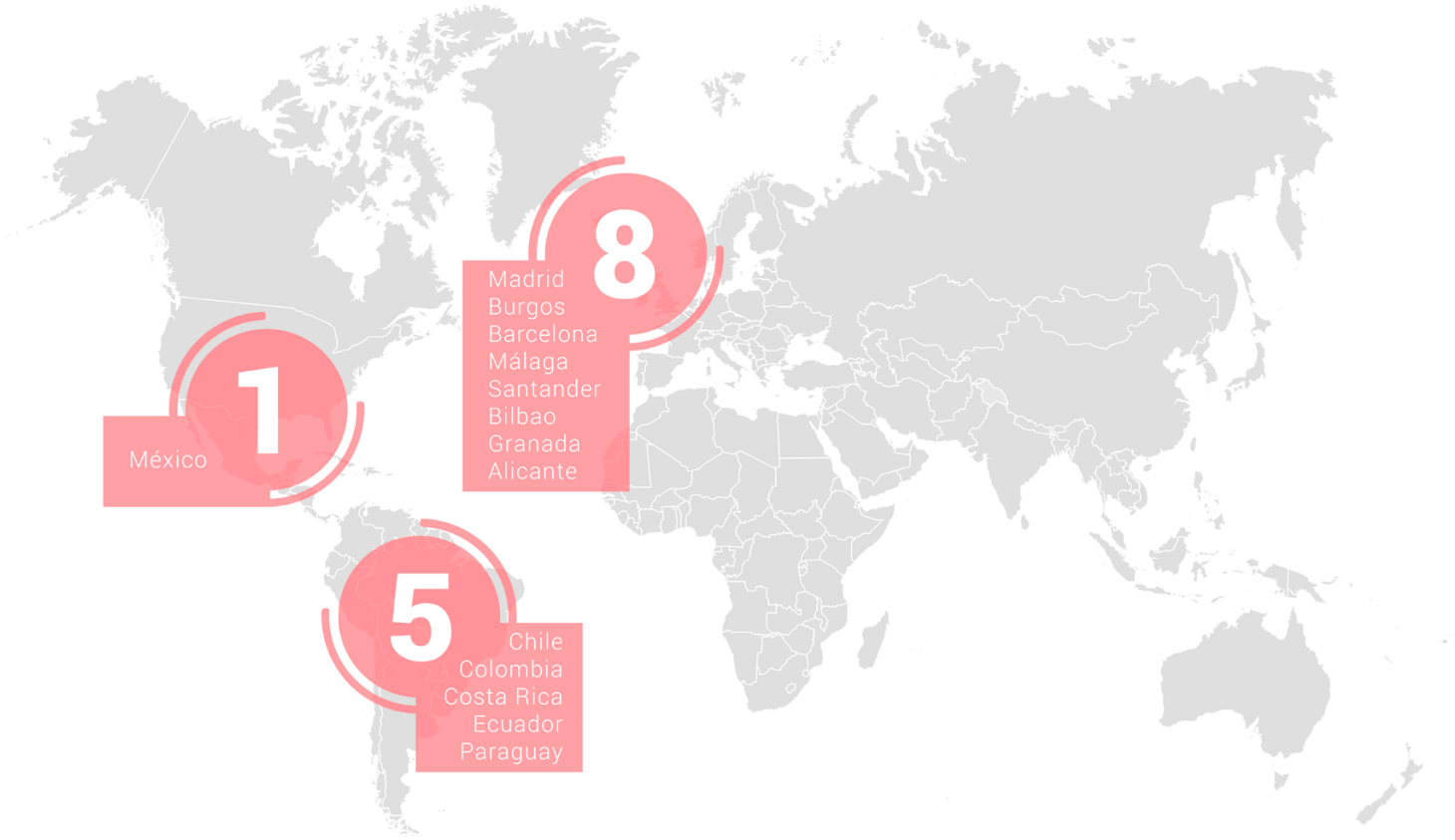
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Informe ENISA Últimas amenazas cibernéticas



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicada el 31/01/2019

En 2018, el panorama de la amenaza cibernética cambió significativamente. Los grupos de agentes de amenaza más importantes, a saber, los ciberdelincuentes y los actores patrocinados por el estado han avanzado aún más sus motivos y tácticas. Los motivos de monetización contribuyeron a la aparición de crypto-miners en las 15 principales amenazas cibernéticas.

También se han evaluado los avances en la defensa: las autoridades policiales, los gobiernos y los proveedores pudieron desarrollar prácticas de defensa activas, como el perfilado de agentes de amenaza y la combinación de inteligencia de amenazas cibernéticas (CTI) e inteligencia tradicional. Esto llevó a una identificación más eficiente de las prácticas de ataque y artefactos maliciosos, lo que a su vez condujo a técnicas de defensa y tasas de atribución más eficientes.

Estamos presenciando el desarrollo y despliegue de nuevas tecnologías, que están cambiando el panorama cibernético e impactando significativamente a la sociedad y la seguridad nacional. La Unión Europea debe estar preparada para adaptarse y aprovechar los beneficios de estas tecnologías para reducir la superficie de los ataques cibernéticos. Este informe crea conciencia sobre los peligros cibernéticos que los ciudadanos y las empresas deben conocer y responder. Ofrece recomendaciones sobre cómo el mercado único digital puede preparar una respuesta adecuada a las amenazas cibernéticas, con la certificación y la estandarización a la vanguardia.

El informe destaca algunas de las principales tendencias relacionadas con las amenazas cibernéticas en 2018:

- Los mensajes de correo electrónico y phishing se han convertido en el principal vector de infección de malware;

- Los cripto-mineros se han convertido en un importante vector de monetización para los ciberdelincuentes;

- Los agentes patrocinados por el Estado atacan cada vez más a los bancos mediante el uso de vectores de ataque utilizados en el ciberdelito;

- La aparición de entornos de IoT seguirá siendo una preocupación debido a la falta de mecanismos de protección en los dispositivos y servicios de IoT de gama baja. La necesidad de arquitecturas genéricas de protección de IoT / buenas prácticas sigue siendo un problema acuciante;

- La inteligencia sobre amenazas cibernéticas debe responder a ataques cada vez más automatizados a través de enfoques novedosos para el uso de herramientas y habilidades automatizadas.

- Las habilidades y la formación son el foco principal de los defensores. Las organizaciones públicas luchan con la retención de personal debido a la fuerte competencia con la industria para atraer talentos de ciberseguridad.

ENISA aborda estas conclusiones haciendo las siguientes recomendaciones:

Política:

- La UE debería desarrollar capacidades para abordar la gestión del conocimiento de CTI. Los Estados miembros de la UE deberían tomar medidas para aumentar su independencia de las fuentes de CTI disponibles actualmente (en su mayoría fuera de la UE) y para mejorar la calidad de la CTI agregando un contexto europeo;

- Los gobiernos de la UE y las administraciones públicas deberían compartir el "CTI de referencia", que cubra las necesidades sectoriales y de baja madurez de las organizaciones;

- La colección de CTI debería hacerse más fácil. Los esfuerzos coordinados entre los Estados miembros de la UE son clave en la implementación de estrategias de defensa adecuadas.

Negocio:

- Las empresas deben trabajar para que la CTI esté disponible para las partes interesadas, centrándose en aquellas que carecen de conocimientos técnicos;

- La industria de software de seguridad necesita investigar y desarrollar soluciones utilizando la automatización y la ingeniería del conocimiento, ayudando a los usuarios finales y las organizaciones a mitigar la mayoría de las amenazas cibernéticas automatizadas de gama baja, con la mínima intervención humana;

- Las empresas deben tener en cuenta las amenazas y riesgos emergentes de la cadena de suministro y cerrar la brecha en el conocimiento de seguridad entre los servicios operados y los usuarios finales del servicio.

Técnico - investigación - educación:

- La gestión de conocimiento de CTI debe ampliarse para incluir información precisa sobre incidentes e información de disciplinas relacionadas;

- La gestión del conocimiento de CTI debe ser objeto de esfuerzos de estandarización, en particular: vocabularios estándar, repositorios de ataques estándar, métodos automatizados de recopilación de información y procesos de gestión del conocimiento;

- Es necesario realizar investigaciones para comprender mejor las prácticas de ataque, la evolución del malware, la evolución de la infraestructura maliciosa y el perfil de los agentes de amenazas.

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com