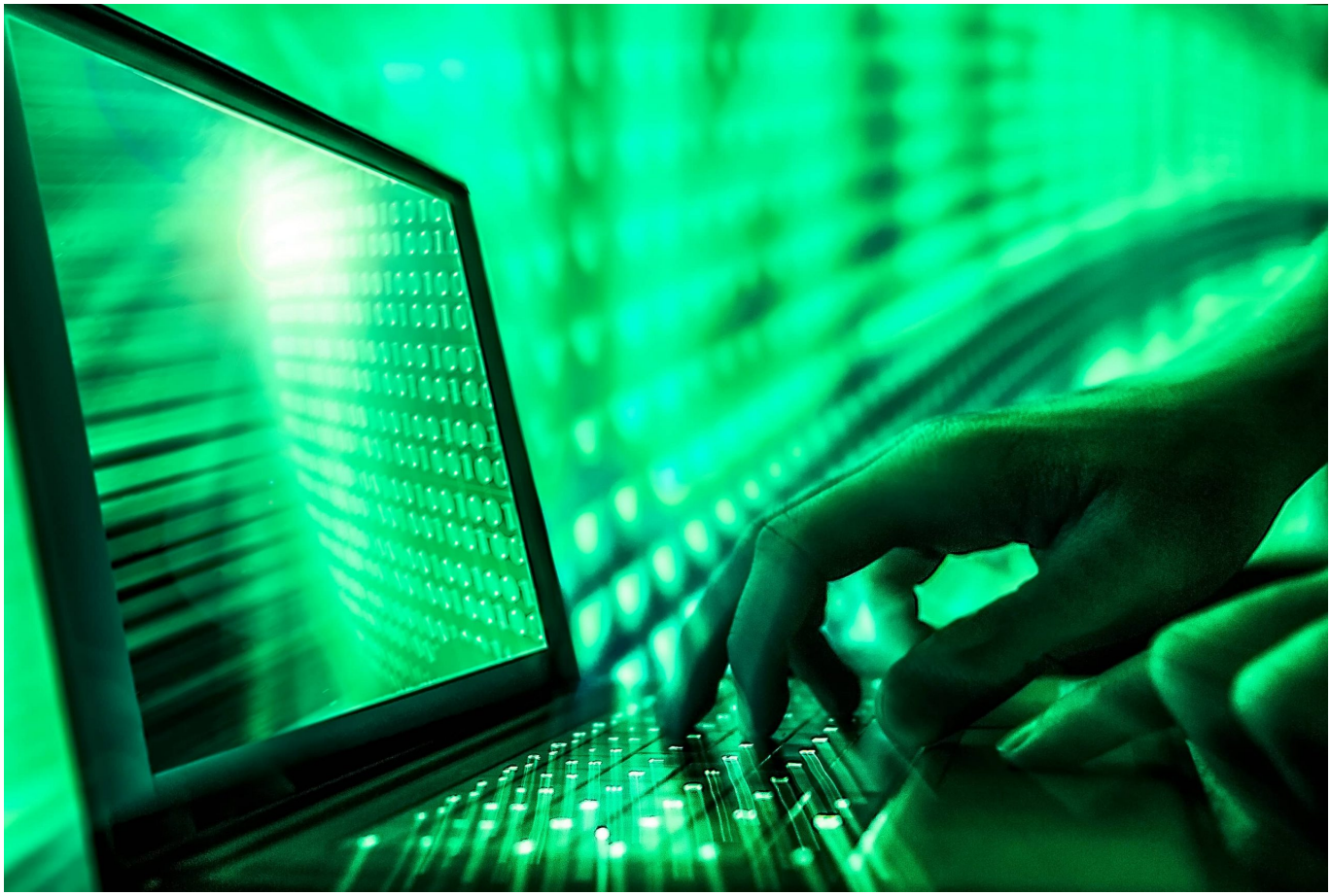
El 97% de las empresas de ciberseguridad han filtrado datos en la Dark Web, según informe

Autor: I. Stepanenko

Fecha: Sunday 27th of September 2020 04:08:51 PM



En un nuevo informe sobre la exposición de la industria de la seguridad cibernética global en la Dark Web este año, la compañía global de seguridad de aplicaciones, ImmuniWeb, descubrió que el 97% de las empresas líderes en ciberseguridad tienen filtraciones de datos u otros incidentes de seguridad expuestos en la Dark Web, mientras que existen en promedio, más de 4000 credenciales robadas y otros datos confidenciales expuestos.

Esta investigación demuestra que hasta la industria de la seguridad cibernética no se salva de los problemas globales relacionados con ataques cibernéticos.

Entre los hallazgos que la investigación encontró relacionados con la exposición de las principales empresas mundiales de seguridad cibernética en la Dark Web, se encuentran:

El 97% de las empresas tienen filtraciones de datos y otros incidentes de seguridad

expuestos en la Dark Web.

Se encontraron 631,512 incidentes de seguridad verificados con más del 25% (ó 160,529) de los clasificados como un nivel de riesgo alto o crítico, que contienen información altamente sensible, como credenciales de texto sin formato, o PII, incluidos datos financieros o similares. Por lo tanto, en promedio, hay 1,586 credenciales robadas y otros datos confidenciales expuestos por cada empresa de ciberseguridad. También se descubrieron más de un millón de incidentes no verificados durante la investigación de ImmuniWeb, y solo 159,462 se estimaron como de bajo riesgo.

El 29% de las contraseñas robadas son débiles, los empleados de 162 empresas reutilizan sus contraseñas. La investigación reveló que el 29% de las contraseñas robadas débiles, cuentan con menos de ocho caracteres o no tienen letras mayúsculas, números u otros caracteres especiales, y que los empleados de 162 empresas reutilizan contraseñas idénticas en diferentes infracciones, lo que aumenta el riesgo de ataques de reutilización de contraseñas.

Se utilizaron correos electrónicos profesionales en sitios de pornografía y citas para adultos. Las infracciones de terceros representaron una cantidad considerable de los incidentes, ya que la investigación de ImmuniWeb encontró 5,121 credenciales que habían sido robadas de sitios web para adultos.

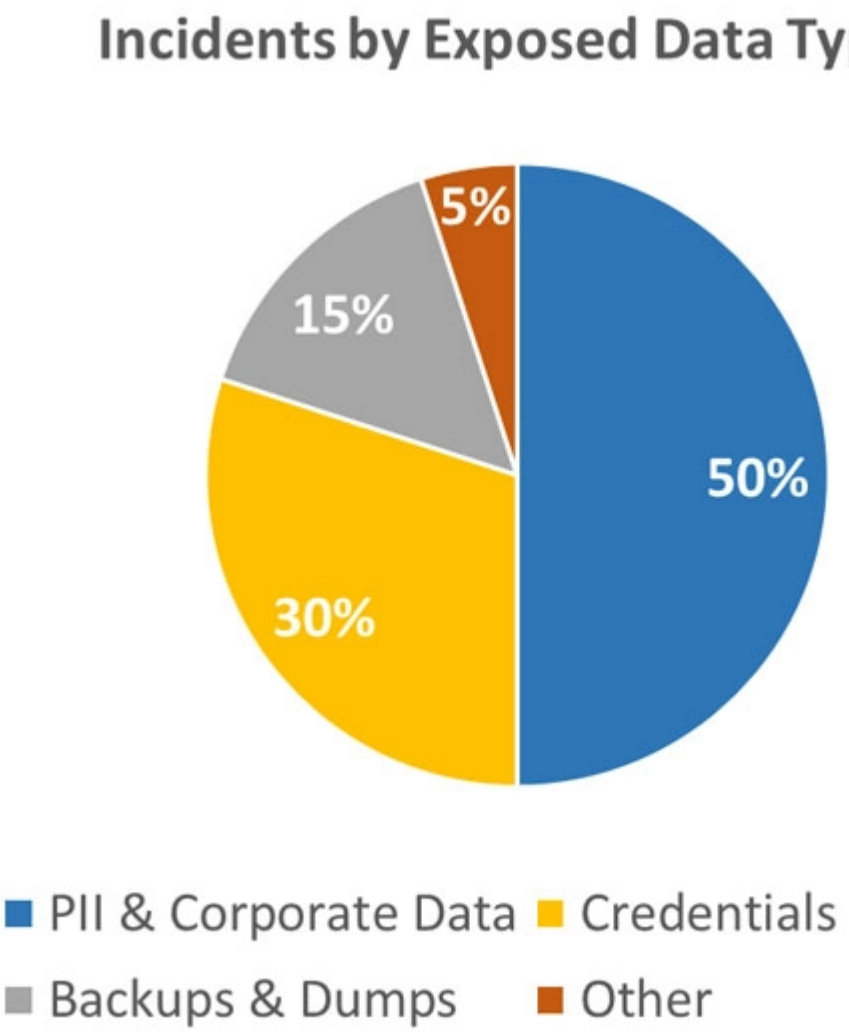
El 63% de los sitios web de las empresas de seguridad cibernética no cumplen con los requisitos de PCI DSS, lo que significa que utilizan software vulnerable o desactualizado (incluidas bibliotecas y marcos JS) o no tienen Web Application Firewall (WAF) en modo de bloqueo.

El 48% de los sitios web de las empresas de ciberseguridad no cumplen con los requisitos del RGPD, debido al software vulnerable, la ausencia de una política de privacidad visible o la falta de una renuncia de responsabilidad de las cookies cuando las cookies contienen PII o identificadores rastreables.

91 empresas tenían vulnerabilidades de seguridad de sitios web explotable, el 26% de las cuales aún no están parcheadas. Este hallazgo se basa en datos disponibles abiertamente sobre el proyecto Open Bug Bounty.

La investigación se realizó utilizando la prueba de seguridad de dominio en línea gratuita de Immuniweb, que combina la tecnología patentada OSINT mejorada con aprendizaje

automático, para descubrir y clasificar la exposición a la Dark Web. Se probaron 398 empresas líderes en ciberseguridad con sede en 26 países, pincipalmente Estados Unidos y Europa.



Las empresas de seguridad cibernética en Estados Unidos sufrieron los incidentes de riesgo más alto y crítico, seguidas por Reino Unido y Canadá, luego Irlanda, Japón, Alemania, Israel, República Checa, Rusia y Eslovaquia.

De las 398 empresas de ciberseguridad probadas, solo las de Suiza, Portugal e Italia no sufrieron ningún incidente de riesgo alto o crítico, mientras que las de Bélgica, Portugal y

Francia tuvieron el menor número de incidentes verificados.

«En la actualidad, los ciberdelincuentes se esfuerzan por maximizar sus ganancias y minimizar los riesgos de ser detenidos al atacar a terceros de confianza en lugar de perseguir a las víctimas finales. Por ejemplo, las grandes instituciones financieras suelen tener formidables recursos técnicos, forenses y legales para detectar e investigar a tiempo, y procesa enérgicamente la mayoría de las intrusiones, a menudo con éxito.

Por el contrario, sus terceros, que van desde bufetes de abogados hasta empresas de TI, por lo general carecen de la experiencia interna y el presupuesto necesario para reaccionar rápidamente al creciente espectro de ataques dirigidos y APT. Con el tiempo, se convierten en frutas fáciles de conseguir para los atacantes pragmáticos que también disfrutan de la tecnología virtual. En 2020, uno no necesita gastar en costotos 0-day, sino más bien encontrar varios terceros desprotegidos con acceso privilegiado a las «joyas de la corona» y romper rápidamente el eslabón más débil.

La visibilidad holística y el inventario de sus datos, TI y activos digitales son esenciales para cualquier programa de cumplimiento y ciberseguridad en la actualidad. Las tecnologías modernas, como el aprendizaje automático y la inteligencia artificial, pueden simplificar y acelerar significativamente una cantidad considerable de tareas laboriosas que van desde la detección de anomalías hasta las falsas reducción positiva. Sin embargo, esta imagen se complementará con un monitoreo continuo de Deep y Dark Web, e innumerables recursos en Surface Web, incluidos los repositorios de código público y sitios web de pegado. No puede desproteger su organización aislada del panorama circundante que probablemente se volverá aún más complejo en el futuro cercano», dijo Ilia Lolochenko, CEO de ImmuniWeb.