COMUNICADO

Gobierno de Gibraltar

El Foro de Reguladores de Gibraltar publica los resultados de una encuesta sobre *ransomware* que pone de relieve la creciente amenaza a la ciberseguridad en Gibraltar

Gibraltar, 4 de octubre de 2024

El Foro de Reguladores de Gibraltar, compuesto por la Autoridad Reguladora de Gibraltar, la Comisión de Servicios Financieros, la Autoridad Reguladora de Servicios Jurídicos, la División de Juego de Gibraltar y la Unidad de Inteligencia Financiera de Gibraltar, ha publicado los resultados de una exhaustiva encuesta sobre *ransomware* , que proporciona información fundamental sobre la prevalencia, el impacto y la preparación de las organizaciones del Peñón ante ataques de *ransomware*. La Encuesta comenzó en junio de 2024 y el análisis de los resultados arroja luz sobre la creciente amenaza del *ransomware*, así como sobre las estrategias de respuesta que se están empleando para combatir estos ataques.

El *ransomware* es un tipo de software malicioso que se ha convertido en una de las amenazas más importantes para los datos, sistemas y redes de todo el mundo. Los delincuentes utilizan el *ransomware* para denegar a las víctimas el acceso a sus propios datos, sistemas o redes y exigen el pago de un rescate para restablecer el acceso. Las tácticas empleadas habitualmente en los ataques de *ransomware* incluyen el cifrado o exfiltración de datos, y la interrupción de sistemas, a menudo acompañadas de amenazas de revelar información sensible.

La Encuesta del Foro de Reguladores de Gibraltar nació con el objetivo identificar el impacto de los ataques de *ransomware* en Gibraltar y comprender cómo las distintas organizaciones se están preparando y respondiendo a estos ataques. El análisis proporciona información sobre las medidas aplicadas, el nivel de preparación y los resultados experimentados por organizaciones que han sido víctimas de ataques de *ransomware*.

Los resultados de la Encuesta suponen ahora una valiosa herramienta para concienciar y orientar a autoridades y organizaciones en la mejora de sus estrategias de ciberseguridad para hacer frente a las vulnerabilidades de forma eficaz. Los detalles no se harán públicos por motivos operativos.

El Foro de Reguladores de Gibraltar reconoce el tamaño limitado de la muestra de la Encuesta y espera aumentarlo en el futuro. No obstante, sus resultados aportan una valiosa visión del estado actual de preparación ante el *ransomware* en Gibraltar, revelando tanto los puntos fuertes como las vulnerabilidades. El Foro de Reguladores de Gibraltar agradece a las organizaciones y personas que han contribuido a la Encuesta y espera poder llevar a cabo nuevas investigaciones en el futuro.

COMUNICADO

Principales resultados de la encuesta

- La mayoría de las organizaciones percibe el *ransomware* como una amenaza significativa, ya que un 79% de los encuestados muestra preocupación, lo que indica que existe un reconocimiento generalizado de los riesgos asociados a los ataques de *ransomware*.

- El 73% de los encuestados considera que son “delincuentes profesionales” los principales responsables tras los ataques de *ransomware*, mientras que el 21% cree que estos ataques están “patrocinados por estados”. Solo el 6% piensa que sus principales autores son “delincuentes novatos”, lo que indica comprensión general de la sofisticada naturaleza de las amenazas del *ransomware*.

- El 80% de las organizaciones de Gibraltar ha designado un departamento o persona responsable de la ciberseguridad, el 68% ha identificado y documentado los riesgos y el 74% ha impartido la formación pertinente al personal. A pesar de estos esfuerzos, solo el 24% tiene una política estricta de no pago en relación con las peticiones de rescate y el 54% no tiene una política oficial.

- Se adoptan medidas preventivas como programas antivirus, procedimientos de copia de seguridad y recuperación de datos y actualizaciones periódicas del software. Sin embargo, casi la mitad de las organizaciones (47%) carecen de un plan formal de respuesta a incidentes, lo que podría dar lugar a respuestas inadecuadas durante un ataque.

- Varias organizaciones de Gibraltar declararon haber sido víctimas de ataques de *ransomware*, y algunas de ellas sufrieron ataques una o dos veces. La mayoría de ellos se iniciaron mediante suplantación de identidad por correo electrónico (email phishing), mientras que otros se debieron a programas informáticos sin parches o a proveedores externos. El impacto de los ataques fue diverso, con pérdidas de productividad, caída de los sistemas y pérdidas financieras. Curiosamente, ninguna organización pagó el rescate y la mayoría pudo recuperar los datos perdidos a partir de copias de seguridad.

- Aunque muchas organizaciones han aplicado medidas preventivas fundamentales, sigue habiendo lagunas en la preparación, particularmente en la planificación de la respuesta a incidentes y en las políticas de negociación de rescate. La variabilidad de las prácticas de ciberseguridad en las distintas organizaciones pone de manifiesto la necesidad de seguir haciendo esfuerzos para reforzar las medidas de ciberseguridad.

COMUNICADO

Nota a redactores:

Esta es una traducción realizada por el Servicio de Información de Gibraltar. Algunas palabras no se encuentran en el documento original y se han añadido para mejorar el sentido de la traducción. El texto válido es el original en inglés.

Para cualquier ampliación de esta información, rogamos contacte con
Servicio de Información de Gibraltar

Miguel Vermehren, Madrid, miguel@infogibraltar.com, Tel 609 004 166
Sandra Balvín, Campo de Gibraltar, sandra@infogibraltar.com, Tel 637 617 757
Eva Reyes Borrego, Campo de Gibraltar, eva@infogibraltar.com, Tel 619 778 498

Web: www.infogibraltar.com, web en inglés: www.gibraltar.gov.gi/press
Twitter: @InfoGibraltar

HM Government of Gibraltar

PRESS RELEASE

No: 637/2024

Date: 4th October 2024

Gibraltar Regulators Forum Releases Ransomware Survey Findings Highlighting the Growing Cybersecurity Threat in Gibraltar

The Gibraltar Regulators Forum, composed of the Gibraltar Regulatory Authority, the Gibraltar Financial Services Commission, the Legal Services Regulatory Authority, the Gibraltar Gambling Division, and the Gibraltar Financial Intelligence Unit, has released the results of a comprehensive ransomware survey (the "Survey"), providing critical insights into the prevalence, impact, and preparedness of organisations in Gibraltar against ransomware attacks. The Survey was launched in June 2024 and the analysis of results sheds light on the growing threat of ransomware, as well as the response strategies being employed to combat these attacks.

Ransomware is a type of malicious software that has emerged as one of the most significant threats to data, systems, and networks worldwide. Criminals use ransomware to deny victims access to their own data, systems, or networks and demand a ransom payment to restore access. Tactics commonly employed by ransomware attackers include data encryption, data exfiltration, and operational disruption, often accompanied by threats to expose sensitive information.

The Gibraltar Regulators Forum Survey aimed to identify the impact of ransomware attacks within Gibraltar and to understand how various organisations are preparing for and responding to such attacks. The analysis provides insight into the measures in place, the level of preparedness, and the outcomes experienced by organisations that have fallen victim to ransomware attacks.

The Survey results now serve as a valuable tool for raising awareness and guiding policy makers and organisations in enhancing their cybersecurity strategies to address vulnerabilities effectively. The granular detail will not be made public for operational reasons.

The Gibraltar Regulators Forum acknowledges the Survey's limited sample size and hopes to grow the size in future surveys. The Survey's results nevertheless provide valuable insight of the current state of ransomware preparedness within Gibraltar, revealing both strengths and vulnerabilities. The Gibraltar Regulators Forum is grateful for those organisations and individuals who have supported the Survey and look forward to conducting further research in the future.

Key Survey Findings

- Ransomware is perceived as a significant threat by most organisations, with 79% of respondents expressing concern indicating that there is widespread acknowledgment of the risks associated with ransomware attacks.

- 73% of respondents view "professional criminals" as the predominant threat actors behind ransomware attacks, while 21% believe these attacks are "state-sponsored". Only 6% think "novice criminals" are the primary actors, indicating a general understanding of the sophisticated nature of ransomware threats.

- 80% of organisations in Gibraltar have designated a department or individual responsible for cybersecurity, 68% have identified and documented the risks, and 74% have provided relevant training to staff. Despite these efforts, only 24% have a strict no-payment policy regarding ransom demands and 54% do not have a formal policy.

- Preventative measures such as antivirus software, data backup and recovery procedures, and regular software updates are well adopted. However, nearly half of the organisations (47%) lack a formal incident response plan, which could lead to inadequate responses during an attack.

- A number of organisations in Gibraltar reported being victims of ransomware attacks, with a few experiencing an attack once or experiencing two attacks. Most attacks were initiated through email phishing, with others resulting from unpatched software or third-party suppliers. The impact of these attacks varied, with productivity loss, system downtime, and financial losses reported. Interestingly, no organisations paid ransom demands, and most were able to restore lost data from backups.

- While many organisations have implemented fundamental preventative measures, gaps in preparedness remain, particularly in incident response planning and policies on ransom negotiation. The variability in cybersecurity practices across organisations highlights the need for continued efforts to strengthen cybersecurity measures.

ENDS