**INTRODUCCIÓN**

Desde sus inicios, las empresas IT (Information Technology) se han visto en la obligación de protegerse de ataques externos cuyo propósito es robar información confidencial, venderla o también cobrar por el rescate de esta. Con la pandemia debido al Covid-19 el espacio de trabajo de estas empresas ha cambiado, creando así un nuevo riesgo de ciberseguridad.

El Ponemon Institute entrevistó 2,215 empleados de TI y seguridad de TI en: Estados Unidos, Reino Unido, Escandinavia, Australia y Nueva Zelanda, donde estos empleados pertenecen a organizaciones cuyas han ordenado migrar al trabajo remoto (Teletrabajo) cuyos resultados arrojaron que en promedio un 22% de las organizaciones, sus empleados trabajaban remotamente; debido al Covid-19, este promedio incrementó a un 58% y a su vez, un promedio del 33% fue despedido.

Los encuestados fueron interrogados acerca de la efectividad de sus correspondientes organizaciones TI, antes y después de la pandemia en una escala del 1 al 10 (1 = poco inefectivo, 10 = muy efectivo), los resultados arrojan que el trabajo remoto ha provocado un decremento en la efectividad de la seguridad de las organizaciones, así como lo muestra la tabla 1.

**Tabla 1:**

**FACTORES CLAVE**

El trabajo remoto ha reducido el costo de las organizaciones, pero no ha hecho a los trabajadores remoto más productivos y eficientes; en la en investigación, el 56% de los encuestados dicen que sus organizaciones esperan que el trabajo remoto sea la nueva norma, debido a esto, se espera que se evalúen los riesgos del trabajo remoto. Sin embargo, de acuerdo con la investigación, el 45% de los encuestados dicen que sus organizaciones no han hecho una evaluación a los riesgos de este espacio de trabajo.

**Tabla 2:** Percepción del impacto por el trabajo remoto en las organizaciones.

Haciendo una conversión rápida:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Trabajar remotamente reduce costos | Trabajo remoto como nueva norma. | Trabajo remoto es eficiente / trabajo remoto más eficiente que el trabajo presencial |
| Encuestados |  |  |  |

Como se puede observar en la gráfica, los encuestados comparten que trabajar remotamente reduce costos y que sus organizaciones tomen el trabajo remoto como nueva norma.

**Información a proteger:** En un ataque a una empresa TI, lo que se busca es robar información confidencial, en la cual destaca más los registros de los clientes (información personal), ya que el objetivo de venderla, es aprovechar la inocencia de los usuarios, y que estos caigan en estafas por internet, entre otros.

De acuerdo con la tabla 3, la información de los clientes es la más vulnerable en la era del trabajo remoto con un 56%, seguido de la información financiera con un 48%.

**Tabla 3: ¿**Qué tipos de información considera que son los más vulneradas en la era del trabajo remoto?

Haciendo una conversión rápida:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Correspondencia de negocios | Registro de empleados. | Propiedad intelectual |
| Encuestados |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Tarjetas de crédito/débito de clientes | Información financiera | Información financiera. |
| Encuestados |  |  |  |

**Tipos de ataques:**

Como se mencionó anteriormente, como resultado del trabajo remoto, muchas organizaciones han visto una disminución en su postura de ciberseguridad. De hecho, el 60% de los encuestados dice haber sufrido un ciberataque; en la tabla 4 se muestra qué tipos de ataques se dieron con más frecuencia.

**Tabla 4:**

Nuestro nuevo total

|  |  |
| --- | --- |
| **Tipo** | **Empleados** |
| Robo de credenciales | 774 |
| Phishing/ingeniería social | 638 |
| Toma de cuenta | 571 |
| Denegación de servicios | 558 |
| Malware general | 558 |
| Ataques basados en web | 478 |
| Malicious Insider | 452 |
| Dispositivos robados/comprometidos | 372 |
| Malware avanzado/zero day attacks | 319 |
| SQL injection | 253 |
| Cross-site scripting | 213 |
| Ransomware | 199 |
| Otros | 66 |

**Ataques por semana:** Los ataques cibernéticos es un factor que las empresas TI tienen que afrontar, sin embargo, ¿qué tan frecuente eran estos ataques durante la pandemia del C19?, los resultados se muestran en la tabla 5.

**Tabla 5:** Cuál fue la cantidad máxima de ataques que tuvo su organización en el lapso de una semana?

Nuestro nuevo total

Teniendo en cuenta estos datos:

**Medidas de tendencia central:**

Mo: 1 ataque/semana

Me: ; 1 ataque/semana

**Conclusión:** Las organizaciones de los encuestados tuvieron aproximadamente entre 1 a 2 ataques por semana, lo cual nos deja en evidencia que las organizaciones no contaban con las suficientes precauciones para poder controlar estos ataques.

**Medidas de dispersión:**

* Varianza:

**Conclusión:** Una varianza de aproximadamente 0.461 indica que los valores tienden a estar relativamente cerca de la media, la cual es 1.587. En otras palabras, la mayoría de los encuestados reportaron un número de ataques por semana que está cerca a la media,

* Desviación estándar

**Conclusión:** La cantidad de "Ataques/Semana" varía en promedio alrededor de 0.679 unidades con respecto a la media de 1.587. Una desviación estándar relativamente baja sugiere que la mayoría de los encuestados reportaron valores cercanos a la media, lo cual permite inferir cierta consistencia en las respuestas de los encuestados.

* Gráfica de dispersión:

**Conclusión:** Con la media y el promedio podemos afirmar quea centralización de los datos (más repetidos), varían de 1 a 2.

**Soluciones:**

* Encriptar los datos sensibles almacenados en los dispositivos.
* Monitorear el tráfico de red 24/7
* Proteger los dispositivos propiedad de la empresa con antivirus, cifrado de dispositivos y firewalls actualizados
* Realizar un proceso de autenticación riguroso para cada empleado de la empresa y de su información personal para evitar el robo de credenciales,

**Conclusiones:**

* A raíz del C19 las empresas TI se vieron afectadas en términos de seguridad por causa del trabajo remoto a lo cual las organizaciones no estaban acostumbradas.
* Los datos arrojados ayudan a buscar soluciones más óptimas a la hora de contrarrestar diversos tipos de ataques cibernéticos.
* Debido a los sucesos de pandemia, desde el ámbito de la investigación se puede tener más claro qué tipo de información se debe proteger y qué tipos de ataque hay que contrarrestar.

**Bibliografía:**

* *Cybersecurity in the remote work era: A global risk report*. (s/f). Keeper® Password Manager & Digital Vault. Recuperado el 20 de octubre de 2023, de https://www.keepersecurity.com/ponemon2020.html