Tendencias y predicciones en el sector de la Ciberseguridad.

Rosa Díaz

Índice

- **Tendencias y predicciones ciberataques 2018.**
- **Marco regulatorio.**
- **Recomendaciones básicas y medidas de seguridad.**

Predicciones ciberataques 2018.

Más ataques esponsorizados por estados

- Estados Unidos, China, Rusia, Israel, Corea del Norte…
- Estados Unidos: 133 equipos en "Fuerza de Cyber Misión" 4.300 personas.
- Todos están aumentando capacidades de sus ciber-ejércitos.
- "*El poder de las ciberarmas no está en la disuasión, el poder de las ciberarmas está realmente en usarlas*". Mykko Hypponen, en Rooted CON.
- Ataques "en directo".
- Ingeniería social más sofisticada.

BEC y BPC

Business Email Compromise y Business Process Compromise.

- Mayor esfuerzo de reconocimiento y de recogida de inteligencia.
- **BEC:** Atacantes se hacen pasar por un alto directivo de la empresa y solicitan una transferencia a un empleado.
- **BPC:** requiere un conocimiento en profundidad de los sistemas de procesamiento de transacciones financieras.
- Ataques contra sistemas de procesamiento de pagos, entregas, soporte técnico, etc.


Inside the TalkTalk 'Indian scam call centre'

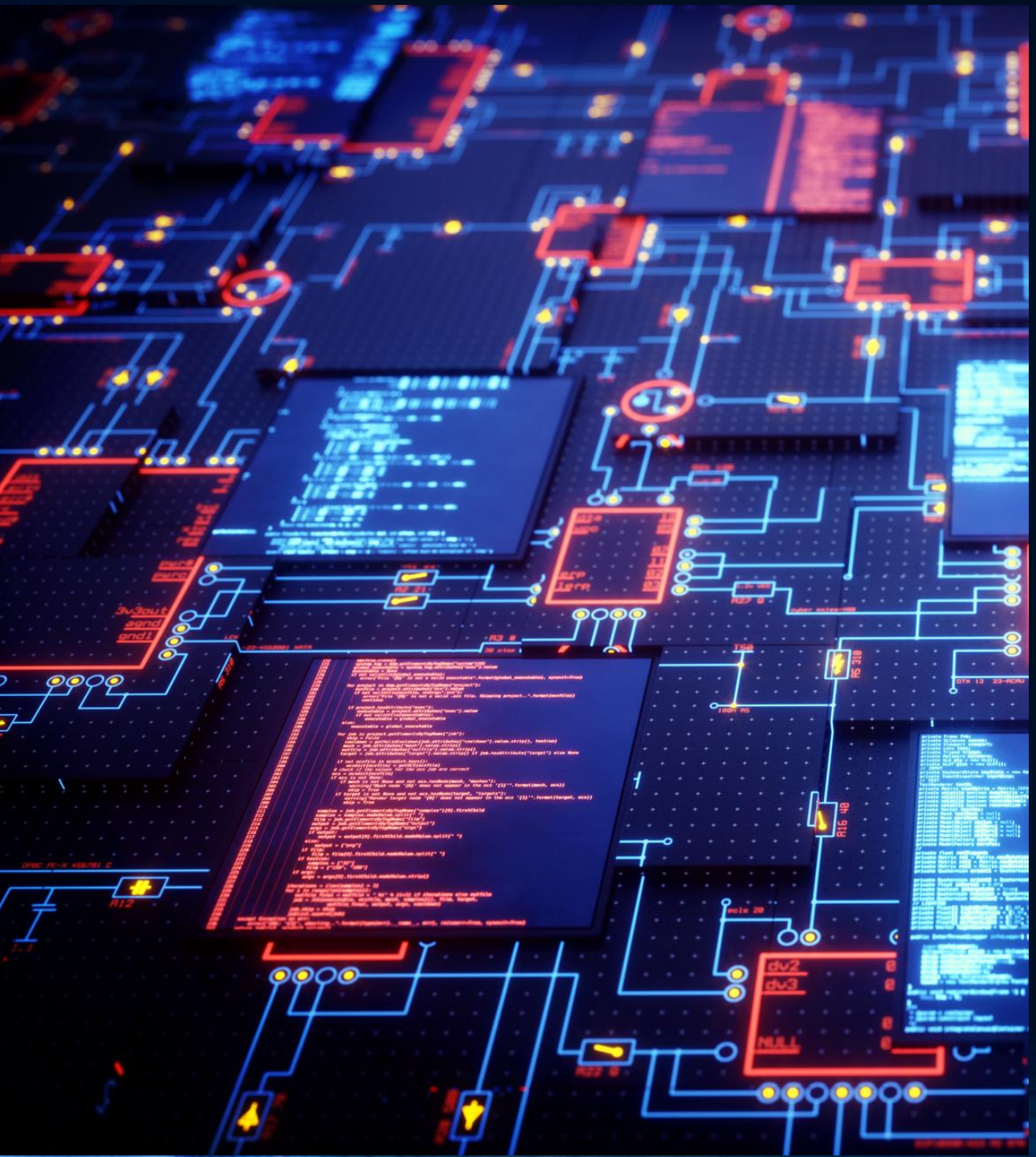
By Geoff White
Technology reporter

6 March 2017 | Technology

El Ransomware evoluciona

- Principal amenaza visible para muchas empresas.
- Evolucionará hacia la nube, móviles, sistemas industriales.
- Posiblemente llegue a su tope este año.
- Muchas variantes.

200.000
nuevo malware/día



Y algunos más…

Ataques sin fichero , sin malware.

Ataque a las Criptomonedas:

- A nivel Micro (Wallets)
- A nivel Macro (Estados y EEFF)

Uso de la IA en redes sociales.

Insiders:

- Malintencionados
- Negligentes

Marco regulatorio.

Marco Regulatorio

1. GDPR
    - Naturaleza muy distinta a LOPD.
    - Implantar métodos de protección.
    - Obligación de Informar (Colaboración).
    - Formación y concienciación.

2. NIS
    - Estrategia Nacional de Seguridad.
    - Cooperación entre estados.
    - Equipos de respuestas a Incidentes.

https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

Recomendaciones básicas y medidas de seguridad.

Recomendaciones básicas y medidas de seguridad

Los básicos:

1. Formar e informar a nuestros colaboradores.
2. Mantener actualizados los sistemas operativos y programas de todos los dispositivos de la empresa contando con una política de actualizaciones y un control de los equipos disponibles.
3. Realizar copias de seguridad.
4. Tener una política de contraseñas seguras.
5. Tener cuidado con los dispositivos extraíbles.

Consejo: contar con una empresa especialista en ciberseguridad que nos pueda realizar un análisis de riesgo de nuestra compañía y nos asesore sobre el plan y medidas a poner en marcha.

Gracias!

rdiazmoles@gmail.com

@rdiazmoles

+ 34 606 951 246