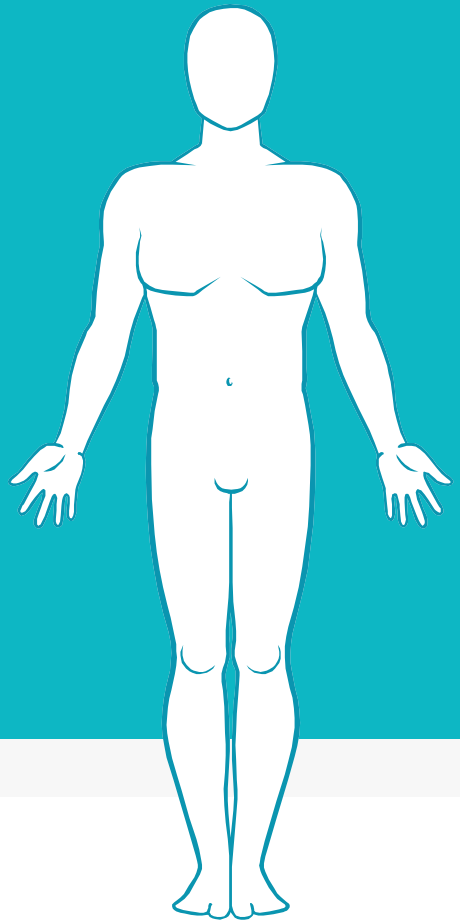
El FACTOR HUMANO EN UN ATAQUE POR RANSOMWARE



Grupo Smartekh

PANORAMA INICIAL

La introducción masiva de tecnologías y las amenazas avanzadas como el Ransomware exigen tomar en cuenta el **factor humano desde una perspectiva de seguridad**.

En la mayoría de los casos los comportamientos inadecuados de los usuarios, el no cumplimiento de las políticas de seguridad y el desconocimiento sobre ciber amenazas pueden hacer blanco de sistemas de operación crítica que pueden exponer la integridad de una empresa.

Los principales **estándares de seguridad** como **ISO 27001** ponen particular atención al argumento donde explícitamente se debe involucrar en el proceso de asegurar la información.

No tiene sentido poseer sofisticados sistemas de seguridad si la seguridad de la infraestructura puede ser potencialmente afectada por el desempeño de seres humanos.

EL ESLABON MÁS DÉBIL

Desafortunadamente en diferentes ocasiones en los ambientes empresariales y de gobierno la seguridad es percibida **como un costo y una carga** que complica la operación diaria.

Grupo Smartekh

3

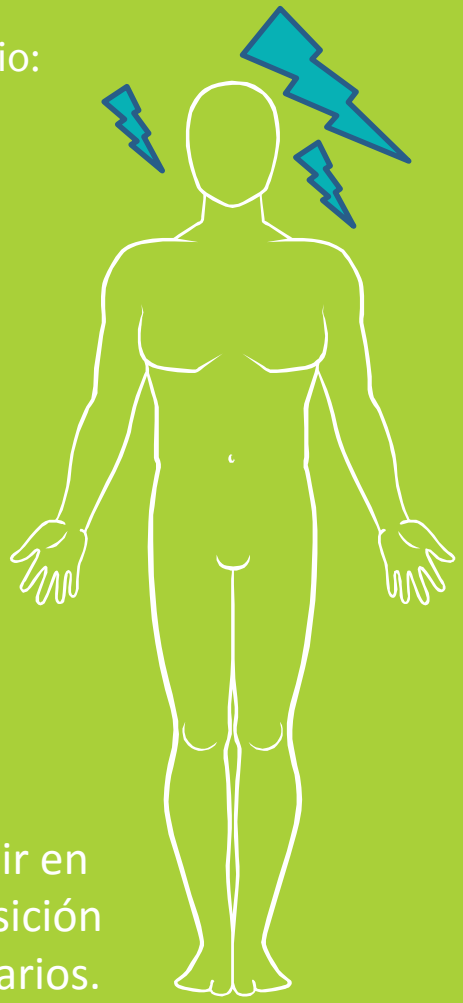
El factor humano es la razón subyacente del porque muchos ciber ataques son exitosos, subestimar la severidad o el potencial de los ataques es uno de los errores más comunes

Analicemos cual es la superficie de ataque actual para cada usuario:

A través de su interacción con:

- Dispositivos móviles
- Accesos inalámbricos
- Laptops
- Equipos de cómputo en nube
- Redes sociales, etc.

> “Todos en conjunto conspirando para hacer la vida más complicada.



Distracción Ignorancia Curiosidad

son algunos de los factores que pueden llevar a un

COMPORTAMIENTO DE ALTO RIESGO

100%

¡Ataque exitoso!

por esta razón es crucial

Definir reglas a seguir en situaciones de exposición al riesgo por los usuarios.

EL USO DE REDES SOCIALES

El uso de redes sociales se ha vuelto uno de los **vectores más usados** de ataque por **ingeniería social**.

Desafortunadamente la mayoría de nuestros usuarios **acepta solicitudes de perfiles no validados** e incluso comparte información de todo tipo que los pone en una situación de **riesgo personal** y para la **empresa** donde laboran, siendo evaluados durante mucho tiempo previo para poder ser usados como un medio ejecutor de un ataque tecnológico o de ingeniería social.

SITUACIONES QUE ELEVAN EL FACTOR DE RIESGO

¿Pero cúales son los factores de mayor riesgo?

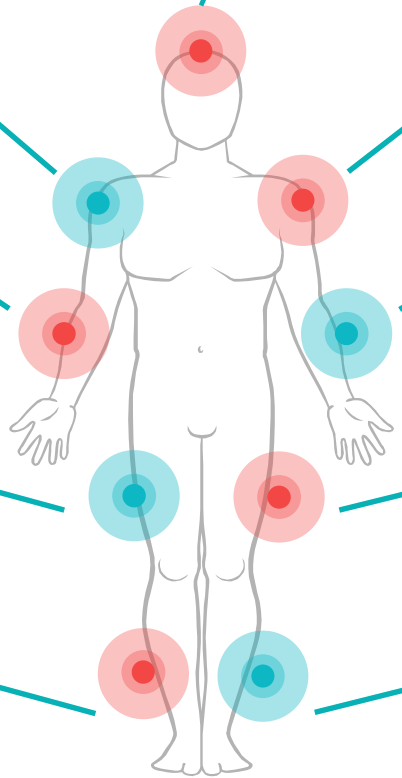
Inadecuada clasificación segmentación de datos

Adopción de un proceso débil de autenticación

Difusión de malware sin conocimiento

Uso indiscriminado de acceso remoto y dispositivos móviles

Deficientes hábitos de respaldo



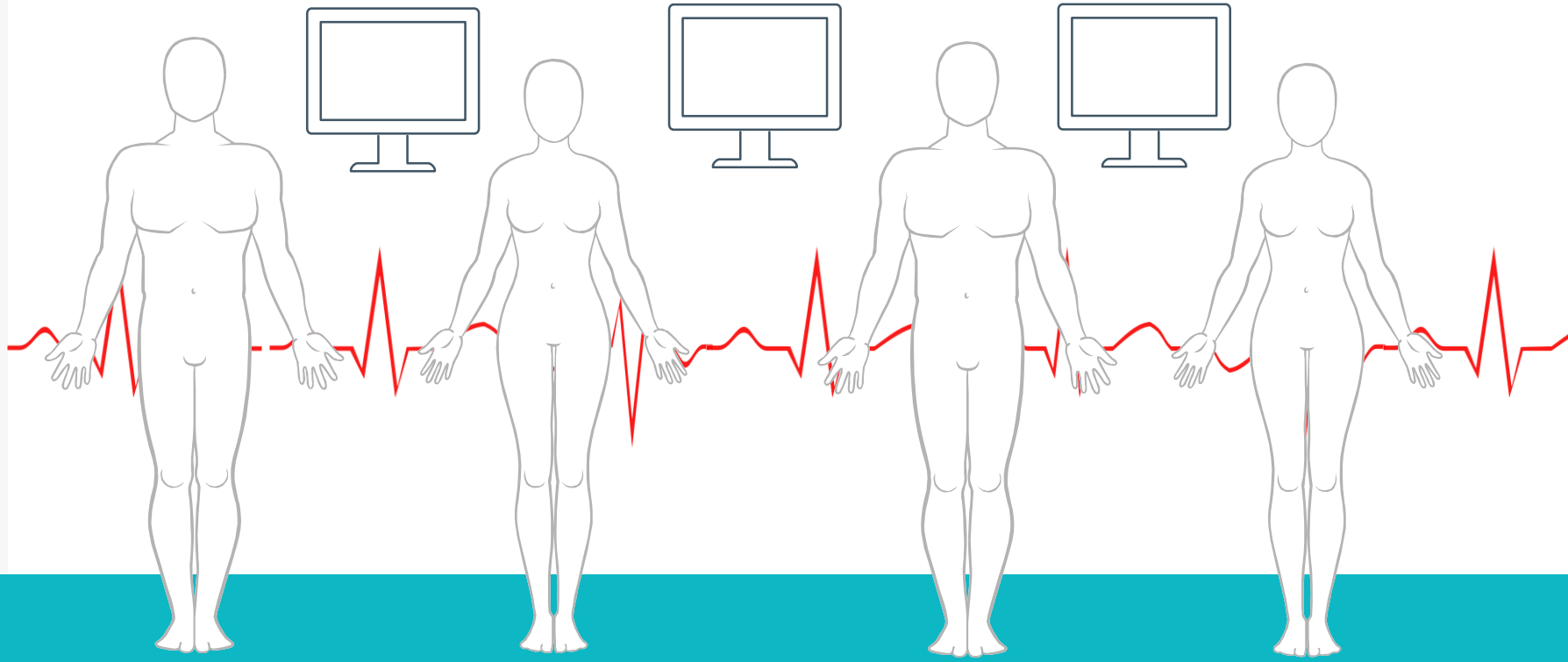
Víctimas de ingeniería social

No aplicación de mejores prácticas al compartir archivos (Boxes, file share etc.)

No adopción de mejores prácticas vs ciber amenazas (tecnología y hábitos)

Conexión a redes Wi-Fi no seguras

El mejor comienzo en una estrategia de seguridad contra Ransomware es un **Diagnóstico Profesional**



¡COMIENZA EL TUYO AQUÍ!

WWW.SMARTEKH.COM

Grupo Smartekh