UTRGV ISO BOLETÍN

www.utrgv.edu/is

The University of Texas Rio Grande Valley

Information Security Office

VOLUMEN I, PUBLICACIÓN VI JUNIO 30, 2017

DENTRO DE ESTA PUBLICACIÓN:

EDITOR

Francisco Tamez

ISO Security Analyst

Jornada calurosa para la Seguridad Informática

¡El verano está finalmente aquí y para muchos de nosotros eso significa que es hora de viajar! El final del semestre de primavera comenzó con varios eventos, uno de estos eventos impactó a 99 países, incluyendo a los Estados Unidos de América. Este verano parece que va a ser una jornada calurosa para la Seguridad Informática.

Por favor siga estos consejos que le guiarán para refrescarle en el verano y con un poco de cuidado es posible protegerse de eventos que puedan impactarlo cibernéticamente.

Viaje con seguridad:

- Actualice sus dispositivos—Verifique que los parches más recientes estén instalados. El proveedor de software debe notificarle cuando haya una actualización disponible.

- Proteja su dispositivo móvil—Instale un buscador de dispositivos en su dispositivo móvil en caso de que lo pierda o sea robado, y si viaja con un dispositivo móvil o portátil, elimine o cifre cualquier información confidencial. Considere la posibilidad de usar un dispositivo móvil designado para viajar sin información personal, especialmente cuando viaja fuera del país.

- Social Media—Evite anunciar en las redes sociales sobre sus planes de viaje y asegúrese de que "No sea SMACKed". Es tentador compartir sus próximos planes de vacaciones con familiares y amigos, pero considere cómo esto podría hacer que usted sea un blanco fácil para los ladrones locales o en línea. Considere la posibilidad de publicar esas hermosas fotos después de regresar a casa.

Sea seguro en línea:

- Asegure su información en tránsito—Mantenga un ojo por el icono de candado en su navegador, o https en la liga (o link)! Estos son los indicadores de que el cifrado está siendo en uso con el sitio.

- Ordenadores públicos y redes inalámbricas abiertas—No acceda a cuentas importantes (como bancos) ni realice transacciones confidenciales en lugares públicos. Por ejemplo: Wi-Fi en aeropuertos, hoteles, cafeterías. Estas redes públicas pueden ser convenientes, pero a menudo no son seguras y pueden dejarlo en riesgo. Cualquier conexión Wi-Fi pública debe ser considerada "no segura".

- Este dos pasos adelante—Active la verificación en dos pasos o la autenticación multifactorial donde se ofrezca para evitar el acceso no autorizado. Esto se puede lograr mediante una combinación de cualquiera de los tres factores a continuación:
  - ◊ Algo que usted sabe - Número de identificación personal (PIN) o Contraseña
  - ◊ Algo que usted tiene - Dispositivo móvil, token o tarjeta de identificación / tarjeta inteligente
  - ◊ Algo que usted es - huella dactilar, retina, patrón de voz

NOTA: El uso de una contraseña en combinación con un PIN, por ejemplo, NO se considera la autenticación de dos factores porque ambas piezas de información implican un solo factor, algo que usted conoce.

AVISOS DE SEGURIDAD

Asegúre su seguridad en la web durante su viaje este verano con una VPN!

El semestre de primavera ha terminado y usted puede estar preparándose para ir de viaje. Si planea conectarse desde el exterior a UTRGV, tendrá que utilizar la red privada virtual (VPN). Hay un par de pasos que deben ser completados antes de salir del campus para asegurar su conectividad. Por favor tómese el tiempo para prepararse y asegúrese de que todos los pasos están completos para estar listo para VPN!

Red privada virtual (VPN) para empleados de UTRGV

El servicio VPN proporciona conexión segura (cifrada) fuera del campus para acceder a los recursos de la Universidad. Utilice VPN para acceder a las funciones de eBusiness de Oracle, como la aprobación de tarjetas de tiempo o el cambio de su información de depósito directo. VPN también se requiere para acceder remotamente a su computadora de oficina y compartir archivos usando Remote Desktop Protocol (RDP).

Usted debe completar las siguientes instrucciones para tener acceso a VPN.

- Inscríbase para la autenticación DUO Mobile de dos factores. **Este paso debe ser completado en la red del campus. Visite utrgv.edu/DUO para inscribirse.**
- Instale la aplicación DUO Mobile en su dispositivo móvil (recomendado).
- Instale el software FortiClient en su computadora, que establece la conexión VPN segura a la red de UTRGV.

Instrucciones de VPN (accesibles con credenciales de UTRGV)

- Conéctese a la red privada virtual (PDF)
- Conéctese a la red privada virtual (iOS iPad)
- Reemplace el dispositivo registrado con DuoMobile para VPN
- Presentación de PowerPoint con audio
  www.utrgv.edu/it/how-to/

¿Saliendo de vacaciones?

Si usted está planeando en sus vacaciones de verano y no va a utilizar su computadora de oficina, entonces no se olvide de apagarlo. ¡Al dejar su computadora apagada usted está protegiendo su información y usted está ahorrando energía al mismo tiempo!

UTPA / UTB Correo Electrónico de Desactivación Permanente el 31 de agosto de 2017

Atención empleados de Legado:

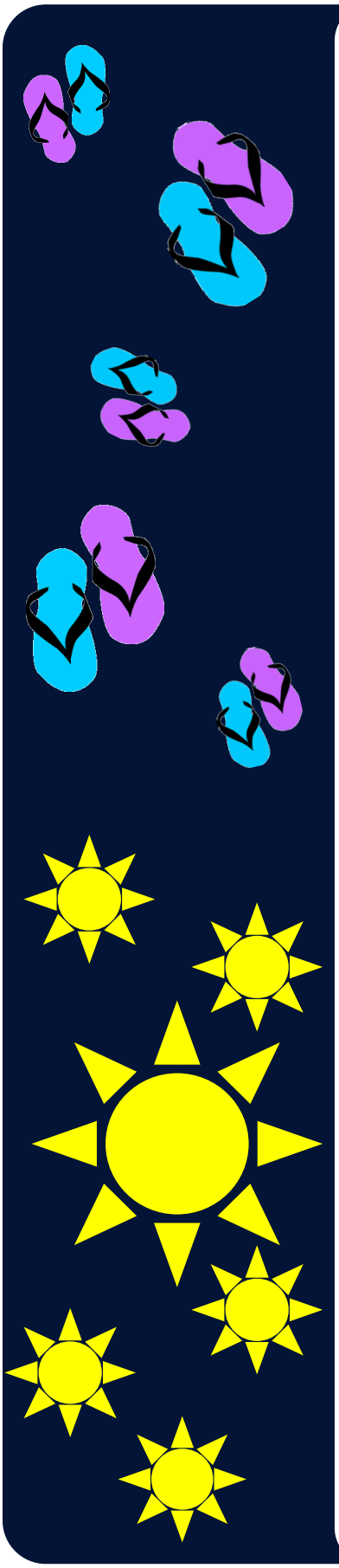
El 31 de agosto de 2017, el reenvío de correo UTPA / UTB (legado) se desactivará permanentemente. Actualmente, los mensajes de correo electrónico enviados a las cuentas UTPA / UTB se envían a las cuentas de correo electrónico de UTRGV. Los mensajes reenviados se indican por su dirección de correo electrónico heredada en la sección "A" del mensaje O incluyen una nota indicando que el mensaje se reenvió desde su dirección de correo electrónico UTPA / UTB.

Usted recibirá amplias notificaciones hasta la fecha de desactivación permanente del 31 de agosto de 2017. Le recomendamos que **tome medidas ahora** e informe a sus contactos que aún utilizan su correo electrónico heredado para usar su dirección de correo electrónico de UTRGV.

Por favor, visite las Preguntas Frecuentes del Sitio Web de IT para obtener más información.

Si tiene alguna pregunta o necesita asistencia técnica, póngase en contacto con el Centro de Servicios de TI:
Brownsville / Harlingen / Isla del Padre
956-882-2020
Main 1212 (Brownsville)

Edinburg / McAllen / Rio Grande City
956-665-2020
Edificio de Servicios Académicos 1.102 (Edinburg)



Software con fin de vida

EOL Software

Las aplicaciones de software tienen un ciclo de vida. El ciclo de vida comienza cuando el software se libera y termina cuando ya no es compatible con el proveedor, también llamado Fin de vida (EOL por sus siglas en inglés). Cuando el software deja de ser soportado por el proveedor, ya no recibe actualizaciones de seguridad.

EOL OS

Windows XP y Apple OSX 10.8 y anteriores son EOL. Si actualmente utiliza uno de estos sistemas operativos (OS por sus siglas en inglés) de EOL, debe actualizar su sistema operativo para mantener la seguridad de su computadora y sus datos. Las computadoras pertenecientes, arrendadas o administradas por UTRGV deben cumplir con el estándar de seguridad informática (bit.ly/UTRUTRGVISOComputerSecurityStandard), que requiere que ejecuten sólo sistemas operativos compatibles con proveedores. Vista será EOL en Abril del 2017, por lo tanto planee actualizar este sistema operativo pronto.

Productos EOL del día de hoy

Actualice si está utilizando los siguientes productos con estas versiones o anteriores.

Producto	Versión	Producto	Versión
Windows	Vista	Adobe Acrobat	9.x
Windows	8.0	Adobe Flash Media	4.5
Adobe Acrobat X	10	Adobe Flash Player	19
Adobe Reader	9.x	Java SE	7
		QuickTime para Windows	

Para actualizar correctamente al sistema operativo más reciente, necesitará los siguientes requisitos de sistema. En el caso de que el hardware del equipo no sea capaz de soportar el último sistema operativo, entonces de acuerdo con el estándar de seguridad informática, el equipo tendrá que pasar por el excedente y una nueva con hardware capaz tomará su lugar.

Si utiliza para su actividad laboral una computadora que es propiedad universitaria con un sistema operativo con EOL, inicie sesión en my.utrgv.edu y envíe un ticket a través de Service Now o póngase en contacto con IT Service Desk lo antes posible.

Brownsville / Harlingen / Isla del Padre Sur 956-882-2020
Edinburg / McAllen / Río Grande City 956-665-2020

Una recomendación amistosa para estudiantes, maestros y empleados de UTRGV que utilizan computadoras personales o portátiles: revise los siguientes requisitos de sistema, inicie sesión en my.utrgv.edu, visite la aplicación vSoftware y compre ($ 9.95 USD) Windows 10; Es muy recomendable que realice una copia de seguridad de todos sus archivos, fotos y otros documentos importantes antes de actualizar su sistema operativo. En el caso de que su computadora personal no sea compatible con el sistema operativo, considere actualizar su máquina.

Para obtener una lista con más software EOL, visite: bit.ly/list-EOL2017

ESCRITORIO LIMPIO

BUENA SEGURIDAD PRÁCTICA

Un ejemplo de mala práctica

Una práctica de escritorio limpio asegura que todos los materiales confidenciales o sensibles se eliminan de un área de trabajo y se ponen bajo llave cuando los elementos no se usan o un empleado sale de su estación de trabajo. Es una de las principales estrategias a utilizar cuando se intenta reducir el riesgo de violaciones de seguridad en el lugar de trabajo. Utilice la lista de verificación a continuación para asegurarse de que su área de trabajo (o hogar) es segura, organizada y compatible.

- ☐ Las contraseñas no deben dejarse escritas en ninguna ubicación accesible.
- ☐ Asegúrese de que toda la información confidencial o sensible en forma impresa o electrónica esté segura al final de la jornada de trabajo o cuando usted se haya ido por un período prolongado.
- ☐ Las pantallas de las computadoras (portátiles, tablets, teléfonos, etc.) deben bloquearse cuando el espacio de trabajo esté desocupado.
- ☐ Los dispositivos portátiles, como las tabletas y teléfonos móviles, deben asegurarse en un lugar bajo llave cuando no se estén utilizando o al final de la jornada de trabajo.
- ☐ Los dispositivos de almacenamiento externo, como los CD, DVD o unidades USB, deben protegerse en un almacenamiento bajo llave cuando no estén en uso.
- ☐ File cabinets, drawers and storage lockers containing Confidential or Sensitive information should be kept closed and locked when not in use or not attended.
- ☐ Llaves utilizadas para acceder información confidencial o sensible no deben dejarse en un escritorio desatendido.
- ☐ Todas las impresoras y máquinas de fax deben ser despejados de los papeles tan pronto como se impriman; Esto ayuda a garantizar que los documentos confidenciales o sensibles no se dejan atrás para que la persona equivocada los recoja.
- ☐ Tras la eliminación*, los documentos confidenciales y / o sensibles deben ser triturados o colocados en contenedores confidenciales bajo llave.

**Aseúrese de que las políticas de gestión y retención de registros de UTRGV se sigan al deshacerse de cualquier registro oficial de UTRGV [HOP ADM-10-102]*

ISO destacó a:

ISO destacó a: es una entrevista de un individuo que forma parte de UTRGV o juega un rol en la seguridad informática. En este boletín, conoceras a Ramon Hermida *Network Security Analyst III*.

Ramon Hermida

Network Security Analyst III,

1. Díganos cómo ha cambiado la seguridad de la información desde que empezó en su papel.
Seguridad de la información como un campo se ha convertido en más maduro y bien definido. Esto tiene que ver con los adversarios que calculan cómo monetizar sus ataques, pero también tiene que ver con la omnipresencia de Internet y la tecnología se han convertido en nuestra sociedad. Seguridad de la información, y la falta de ella, se encuentran dondequiera que observe el día de hoy. Esto es siempre tan evidente cuando los atacantes realizan un ataque de denegación de servicio. Por ejemplo, en el servidor de Minecraft que su hijo de 10 años está diseñando su obra maestra de barro.

2. ¿Cómo es que llegaste al campo de seguridad informática?
Recuerde que a principios de los años 2000 no había mucho en el "campo de seguridad". Mi primer título de seguridad "oficial" fue en 2005 con la universidad. En trabajos anteriores, siempre estaría involucrado con algún aspecto de Seguridad de la Información. Mi primera experiencia memorable con la Seguridad de la Información, y cómo los ataques devastadores pasaban, sucedió en 2001. Nadie en la empresa entendió lo que estaba trayendo a los controladores de dominio, incluyendo varios consultores. Había alrededor de 80 empleados de tiempo completo, simplemente sentados ahi, sin poder acceder a sus cuentas y trabajar. Lo que me llamó la atención fueron algunas entradas anormales en mis servidores Linux, que más tarde se reveló que eran la tarjeta de llamada del gusano Code Red.

3. Los tres logros mas importantes en su vida:

- Reubicarme en Texas con prácticamente cualquier cosa que podia empacar en un avión
- Casarme con Irma
- Una comprensión más profunda de la vida a través de prácticas meditativas

4. La gente se sorprendería saber que:
He montado mi bicicleta de Houston a Austin. Siempre monto una bicicleta cada vez que viajo. Tengo una meta para montar mi bicicleta en cada estado, y tantos países como pueda.

5. ¿Qué CD tiene usted en su coche? ¿O qué estación de radio te gusta escuchar?
De hecho, no tengo coche. Sin embargo, soy un firme creyente en la escucha de generadores de ruido de fondo y binaural beats. Por ejemplo, busca en Google “NOISLI” para obtener una mejor comprensión a lo que me refiero. Y no, no me pagaron para decir eso.

6. Si pudieras entrevistar a una persona (viva o muerta) ¿Quién sería?
Albert Einstein. No tanto para hablar de física o relatividad, sino para comprender su perspectiva general en la vida. Cosas como: ¿A qué hora se levantaba todos los días? ¿Cuáles eran sus rituales diarios? ¿Cuáles fueron sus metas de vida? ¿Qué pensaba que era su propósito de vida? ¿Cómo gestionó los proyectos y los plazos en el trabajo? ¿Cómo logró manejar su equilibrio trabajo-vida?

7. ¿Cuál es el mejor consejo que has recibido y que ha utilizado?
El consejo que me dio mi profesor de inglés en la preparatoria. Quería que tomara clases de AP, en lugar de clases regulares. Naturalmente, negué. A lo que su respuesta fue: "evalua cuál de las opciones y la dirección en la que puedes fácilmente caer de nuevo, y elige la más difícil (y a menudo suele ser la más gratificante)". Así que en este ejemplo, podría tomar las clases de AP, y si caia, podría fácilmente tomar los cursos regulares. Sin embargo, ir en la otra dirección no habría sido tan fácil, o gratificante.

8. ¿Cuál sería su consejo para un nuevo profesional en la seguridad informática?
Siempre nutrir un nivel saludable de la curiosidad y obtener experiencia práctica en cualquier aspecto de la Seguridad de la Información que quieras estar involucrado, o desees estar involucrado. Tenga en cuenta que nuestro campo está en constante flujo, y que usted tendrá que obtener esta experiencia fuera del trabajo o la escuela. He visto un montón de gente con un titulo en seguridad de la información y son incapaces de responder a las preguntas básicas de seguridad.

WannaCry Ransomware and Lessons

De: Departamento de Recursos de Información
DIR.texas.gov

Una vulnerabilidad descubierta por primera vez por la Agencia de Seguridad Nacional y luego liberada por hackers en el Internet se utiliza ahora en uno de los ciberataques más prolíficos de todo el mundo.

El 12 de mayo de 2017, los blogs de tecnología y las noticias se encendieron con el nuevo ataque de ransomware que se propagaba como un reguero de pólvora a través de redes públicas y privadas, bloqueando a la gente de sus datos y exigiendo que pagaran un rescate o perdieran todo. Agencias como el British National Health Service (NHS) y Telefonia, el mayor proveedor de telecomunicaciones de España, fueron afectadas. Incluso empresas privadas como Fedex sintieron el peaje de este software malicioso. Sólo en las primeras horas, entre 230.000 y 390.000 ordenadores en más de 150 países se infectaron con este ransomware recién descubierto. Su nombre era WannaCry (WNCRY / WannaCrypt).

Este ataque nos enseñó algunas lecciones difíciles.

1. **Parche…. ¡PARCHE!** Todo el mundo siempre lo dice pero claramente no todo el mundo lo hizo. Este ransomware atacó con éxito tantos sistemas debido a sistemas operativos no soportados o sin actualizaciones.

2. **El olvido no es excusa.** Los sistemas dejados en el pasado a menudo significan puntos de acceso no monitorados. WannaCry demostró que importante es la gestión consistente de los activos. Los malos actores se aprovechan de tu error humano. Es fundamental dar un paso atrás y observar su sistema desde el exterior. Si estuviera tratando de colarse en sus sistemas, ¿dónde buscaría primero?

3. **Construir muros con segmentación de red.** Parchar y actualizar viejos sistemas a menudo viene con una serie de desafíos técnicos. Por esta razón, los nuevos sistemas a menudo se construyen en la parte superior de los antiguos. Muchos no se dan cuenta del riesgo de los sistemas sin parches y la falta de segmentación de la red. La segmentación de la red y la arquitectura de red bien planificada podrían haber salvado a algunas organizaciones un mundo de dolor.

4. **La ciberseguridad protege la vida real.** Es importante recordar, mientras que la ciberseguridad es digital y usted puede estar luchando la buena lucha detrás de una pantalla de computadora, la vida de la gente cuelga en la balanza. El ataque de WannaCry a los servicios de atención de salud en el Reino Unido, fue una muestra clara de que hay consecuencias que van mucho más allá de bitcoin.

5. **¡No olvide la disponibilidad!** WannaCry dio a las organizaciones una golpe rápido en la parte trasera y les recordó que la disponibilidad en dentro de la rama de la CIA (Confidencialidad, Integridad y Disponibilidad) es esencial para el éxito de los negocios cotidianos. El costo de este ransomware se estima en más de $ 8 billones de dólares debido a la interrupción del negocio, la pérdida de ingresos y el tiempo invertido en la restauración.

ISO Invitado

Salud Ambiental, Seguridad y Gestión de Riesgos

Gestión y eliminación de residuos peligrosos, biológicos y radiactivos

Las baterías se manejan como "Residuos Universales" y tenemos un programa para reciclar baterías específicas que incluye lo siguiente:

A. Baterías de plomo ácido (baterías de coche)
B. La mayoría de las baterías recargables (por ejemplo, NiCad)

Note: Las baterías de uso común, incluyendo alcalinas (AA, AAA, C, D, 9 voltios) no son peligrosas y pueden ser desechadas con residuos sólidos (basura) sin requisitos especiales.

Los toners tampoco son peligrosos y pueden ser desechados con basura regular, pero también tenemos un programa de reciclaje para minimizar el impacto en nuestros vertederos.

Los departamentos que generan estos dos tipos de residuos pueden enviar una solicitud de recogida a waste@utrgv.edu, las recolecciones de estos artículos se realizan generalmente los viernes.

UTRGV Safety
Is In Everybody's Job Description

Office of Emergency Preparedness Contact Information

Phone: (956)665-3690
Email: EHSRM@utrgv.edu
Website: www.utrgv.edu/ehsm


DON'T
GET
SMACked
Check your
Social Media
Access Controls
utrgv.edu/is/en-us/
resources/social-media


WE
ARE
SOCIAL!
www.utrgv.edu/is
www.facebook.com/utrgviso

ARTÍCULOS DE SEGURIDAD

1 millón de usuarios de Gmail afectados por Google Docs Phishing Attack

"Pudimos detener la campaña en aproximadamente una hora", dijo un portavoz de Google en un comunicado. "Aunque la información de contacto fue accesada y usada por la campaña, nuestras investigaciones muestran que no se expusieron otros datos. No hay más acción que los usuarios tengan que tomar con respecto a este evento ".
bit.ly/googlephishingattack

Chipotle incumple restaurantes afectados en 47 estados

Poco después de Chipotle informó de una violación el 25 de abril que afectó a más de 2.000 locales de restaurantes y un número no revelado de personas en 47 estados, una investigación concluyó el punto de venta (POS) malware ataque duró del 24 de marzo al 18 de abril y buscó "Datos de pista" que a veces incluye números de tarjeta, fechas de vencimiento y códigos de verificación internos, según la alerta de seguridad de Chipotle.
bit.ly/chipotlebreach2017

Archivos sensibles del Pentagono en el servidor de Amazon sin contraseña

Un caché de más de 60.000 archivos fue descubierto la semana pasada en un servidor de Amazon públicamente accesible, incluyendo contraseñas a un sistema del gobierno de los Estados Unidos que contiene información confidencial y las credenciales de seguridad de un ingeniero principal.
Además, aproximadamente 28 GB de datos contenían al menos media docena de contraseñas no cifradas pertenecientes a contratistas gubernamentales con Top Secret Facility Clearance.
bit.ly/pfileswnopassword

SANS OUCH! Boletín de Junio: Lecciones que podemos aprender de WannaCry

Recientemente, es probable que hayas visto una tremenda cobertura informativa de un nuevo ataque cibernético llamado "WannaCry". Este malware infectó más de 200,000 computadoras, bloqueando los datos de varias organizaciones, incluyendo hospitales en el Reino Unido.

Hay varias razones por las que este ataque generó tanta atención. En primer lugar, se extendió rápidamente de una computadora a otra atacando una debilidad conocida en computadoras con sistema Windows. En segundo lugar, el ataque fue un tipo de malware llamado "ransomware", lo que significa que una vez que infectó tu computadora cifró todos tus archivos, bloqueando tus datos. La única manera de recuperar los datos es mediante copias de seguridad o pagando al atacante un rescate de $300 USD para descifrar los archivos. En tercer lugar y el más importante, este ataque nunca debió haber sucedido.

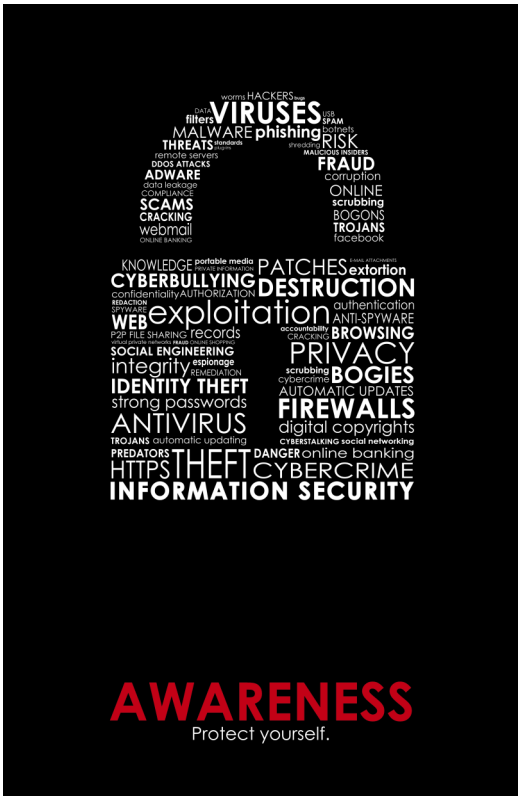
La debilidad que WannaCry atacaba en computadoras con sistema Windows era bien conocida por Microsoft, que había lanzado una corrección meses antes. Pero muchas organizaciones no pudieron instalar la corrección, o todavía usaban sistemas operativos como Windows XP que son tan viejos que no hay ningún parche disponible.
securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201706_sp.pdf

Los hackers alojaron herramientas en un sitio web de la Universidad de Stanford durante meses.

La conmoción de sitios web legítimos y los servidores web que los almacenan y entregan es una táctica consagrada de hackers oportunistas, y un fracaso en mantenerlos fuera puede provocar que los servidores hospeden páginas de phishing y estafa. Spam, kits de explotación o malware.
bit.ly/hackerstoolsstanforduni

La infracción de datos en la Universidad de Oklahoma afecta a 30.000 estudiantes

La falta de configuración de privacidad en una red de intercambio de archivos del campus llevó a una exposición no intencional de los registros educativos de miles de estudiantes en la Universidad de Oklahoma.
bit.ly/databreachOklahomaU



Si necesitas reportar un incidente:

Visite nuestro sitio web (www.utrgv.edu/is) si necesita reportar un incidente de seguridad . Algunos incidentes pueden requerir informar tanto a la ISO y al Departamento de Policía de UTRGV (PD) o de tecnología de la información (IT) . Por ejemplo, cualquier pérdida o robo de una computadora de propiedad de la Universidad (ej. estación de trabajo, ordenador portátil, celular, tableta) tiene que ser reportado a la ISO y a UTRGV PD. Del mismo modo, en caso de computadoras infectadas con ransomware deben de ser reportadas a ISO y a IT.

REPORTA UN INCIDENTE

The University of Texas Rio Grande Valley™

Information Security Office

The mission of the Information Security Office is to provide support to the University in achieving its goals by ensuring the security, integrity, confidentiality, and availability of information resources. The role of the Chief Information Security Officer (CISO) is to maintain oversight and control of the enterprise information security program for the University.

Locations:

- Sugar Road Annex (ESRAX) Building
- R-167 Rusteberg Hall (BRUST) Building (*by appointment*)

Phone: (956)665-7823

Email: is@utrgv.edu

Visit us on the web and social media!
www.utrgv.edu/is www.facebook.com/utrgviso

Services We Provide

GOVERNANCE, RISK AND COMPLIANCE

ASSET AND VULNERABILITY MANAGEMENT

ENGINEERING AND INCIDENT RESPONSE

AWARENESS, COMMUNICATION AND OUTREACH

Danos tu FEEDBACK!
bit.ly/utrgvisonewsletterfeedback

Agradecimiento a:

Information Technology

Irma Hermida and Hilda Gonzalez

Environmental Health, Safety & Risk Management

Dr. Richard Costello and Liza Dimas