ISO
BOLETÍN

www.utrgv.edu/is

The University of Texas Rio Grande Valley™
Information Security Office

VOLUMEN I, PUBLICACIÓN I SEPTIEMBRE 02, 2016

DENTRO DE ESTA PUBLICACIÓN:

EDITOR
Francisco Tamez
ISO Security Analyst

Bienvenido al semestre de Otoño 2016

La Oficina de la Seguridad Informática (ISO por sus siglas en inglés) se enorgullece en presentar su boletín inaugural. Este boletín bimensual se esforzará para mantenerlo informado acerca de noticias de seguridad importantes y temas que le ayudarán a permanecer seguro tanto en el trabajo (para los empleados), en la escuela (para los estudiantes), o en casa (para todos). Sus comentarios, ideas y críticas son bienvenidas. Esperamos que este boletín mensual sirva a la comunidad de UTRGV de la mejor manera posible. Bienvenido al semestre de Otoño 2016 y el comienzo de otro gran año académico !

Algunos recordatorios básicos de seguridad para ayudarle a iniciar el nuevo semestre de otoño:

1. Mantenga su software de ordenador actualizado. Compruebe que su sistema operativo (SO) tiene la actualización más reciente, así como cualquier otra aplicación que haya instalado, especialmente los lectores de Adobe, los navegadores web (Internet Explorer, Edge, Safari, Chrome, Firefox, etc.) y productos de oficina (Word, Excel, etc.)
2. No se olvide de actualizar su antivirus y ejecutar un escaneo completo al menos una vez al mes. Usted no necesita gastar su dinero para mantenerse protegido, hay muchos productos de antivirus disponibles de forma gratuita! El uso de un ordenador sin protección contra virus es como conducir un coche sin parabrisas en la carretera, estas desprotegido y es muy probable que algo te dañara. (Http://bit.ly/25BuJ7i)
3. Revisa tu correo electrónico de UTRGV - hoy en día la mayoría de los profesores y compañeros de clase van a comunicarse a través de correo electrónico. Los empleados de UTRGV deben utilizar su correo electrónico para realizar negocios oficiales de la universidad.
4. No caigas en Phishing- al hacer clic en enlaces webs en correos electrónicos y descargar archivos adjuntos que no esperabas o si simplemente hay algo que no está bien, ¡no lo abras! Podría ser un intento de phishing.
5. Utilice contraseñas seguras para todas sus cuentas. Deben tener al menos 14 caracteres y contener letras mayúsculas y minúsculas, números y símbolos. Utilice contraseñas diferentes para cada una de sus cuentas. No utilice las contraseñas de sus operaciones bancarias o de UTRGV en sitios de redes sociales. Un buen gestor de contraseñas puede ayudarle a mantener buen control de todas sus contraseñas. (Http://bit.ly/2aEeO6i)
6. Minimice (o elimine) el uso the USB para transferir datos entre computadoras. Debido a que fácilmente pueden ser perdidos o robados y en veces estos USB fallan. Se les ha dado a todos los usuarios de UTRGV una cuenta de Microsoft OneDrive, se recomienda que se utilice en vez del USB.

ANUNCIOS

EOL Software

Las aplicaciones de software tienen un ciclo de vida. El ciclo de vida comienza cuando el software es anunciado y concluye cuando ya no es soportado por el proveedor, también llamado fin de vida (EOL por sus siglas en inglés). Cuando el software deja de ser apoyado por el proveedor, instantáneamente deja de recibir actualizaciones que permite mantener el software seguro.

EOL OS

Windows XP y Apple OSX 10.6 y versiones anteriores son EOL. Si actualmente está utilizando un sistema operativo EOL, debería actualizar su sistema operativo para mantener la seguridad de su equipo y sus datos. Ordenadores en propiedad, arrendados o gestionados por UTRGV deben cumplir con la Norma de Seguridad Informática, el cual requiere que se ejecuten solamente sistemas operativos que sean apoyados por el proveedor. Windows Vista será EOL en abril de 2017, planeé actualizar este sistema operativo pronto.

QuickTime EOL

Apple anunció que ya no lanzará soporte para QuickTime para Windows. Las computadoras con el sistema operativo de Windows y que están utilizando QuickTime pueden ser vulnerables al malware. ISO recomienda que todos los usuarios de Windows desinstalen QuickTime.

PowerBroker

Durante todo el verano la Oficina de la Seguridad Informática (ISO) y Tecnología de la Información (IT) (ISO, IT por sus siglas en inglés) han implementado una solución de acceso privilegiada llamada PowerBroker para todas las computadoras que pertenecen a UTRGV. La solución PoweBroker ya se ha lanzado en todos los equipos con Windows. Computadoras con Apple OS X pueden solicitar PowerBroker mediante una solicitud de servicio con IT Service Desk. PowerBroker es una aplicación que permite a los empleados de UTRGV realizar tareas administrativas, tales como la instalación y actualización de software, adición o eliminación de impresoras, sin necesidad de un acceso privilegiado o asistencia de IT. Para aprender más acerca de PowerBroker, visite cómo utilizar PowerBrower en el sitio web de IT (www.utrgv.edu/it/how-to).

¿Que aguarda este semestre de Otoño 2016?

Octubre NCSAM

Octubre es el mes nacional del consentimiento de la seguridad cybernetica (NCSAM por sus siglas en inglés), administrado por el Departamento de Seguridad Nacional. La Oficina de la Seguridad Informática (ISO) discutirá la seguridad cibernética en varios temas: el uso de programas malignos por los delincuentes en línea, el robo de la propiedad intelectual, el fraude por Internet, el fraude de identidad, acoso cibernético, y mucho más. Nuestra oficina estará proporcionando consejos cibernéticos semanales en Octubre a través de nuestra página web y las redes sociales.

ISA Entrenamientos

La ISO comenzará a buscar a los administradores de seguridad informática (ISA por sus siglas en inglés) para cada departamento. Los ISA actuarán como un conducto entre la ISO y todos los departamentos y facultades. Esto ayudará a construir vías de comunicación para asegurar que los empleados y la ISO son informados de temas y problemas que afectan la seguridad informática.

Proyectos actuales de ISO

Nuestra oficina está trabajando en varios proyectos que mejorarán la gestión de activos y la vulnerabilidad de las computadoras en nuestra Universidad. La ISO está optimizando los métodos de descubrimiento de activos, inventario, la clasificación de los datos, y la prevención de pérdida de datos.

Síguenos en las redes sociales www.facebook.com/utrgviso y visita nuestro sitio web para más información www.utrgv.edu/is

Ransomware: El malo y el feo

Por: Daniel Ramirez (UTRGV Sr. Information Security Analyst)

Lo básico, ¿qué es ransomware? Ransomware es un tipo de malware que se dirige a sus datos y sistemas con el fin de la extorsión. Ransomware se dirige a determinados tipos de archivos como: .doc, .pdf, .xls, .jpeg, .mov, .zip, y muchos otros. Aquellos archivos que contienen datos importantes como fotos personales, videos memorables, proyectos de trabajo importantes, o cualquier dato que un sujeto con malas intenciones (ej. pirata, hacker) pueda determinar aquello que es suficientemente importante para usted y forzarlo a pagar dinero para recuperarlo. Los últimos dos años de fotografías que tú tomaste con tu celular o tu investigación completa del año pasado y que tenías almacenada en tu computadora, ¡todo se puede perder en un instante!

Javier Jaén

Ransomware es frecuentemente entregado a través de correos electrónicos maliciosos, donde aquellos sujetos con malas intenciones te engañan en abrir un documento infectado o haciendo click en un link que te llevara a un sitio web infectado. Aquellas computadoras sin antivirus o con software que no está actualizado pueden ser infectadas muy fácilmente por ransomware (y otro malware). Una vez que la computadora es infectada con ransomware, el ransomware va a atacar archivos específicos en la computadora de la víctima y los bloqueara con cifrado, bloqueándolos al punto donde ni siquiera el dueño de los documentos los puede acezar. Después de que el usuario ha sido bloqueado de los datos, el ransomware va a mostrar una notificación donde informara a la víctima que los archivos ahora están retenidos como rehenes, cuanto te costara para recuperarlos y cuanto tiempo para que los archivos sean perdidos para siempre. Después de que el ransomware reciba el pago, aquellos sujetos con malas intenciones supuestamente van a proporcionar una vía donde la victima podrá recuperar el acceso a los datos

Javier Jaén

Ransomware es el malware que a crecido más rápido, atacando usuarios de todos tipos, desde el usuario en casa hasta una red corporativa. En promedio, más de 4,000 ataques de ransomware han ocurrido diariamente desde Enero 1, 2016. Esto es un crecimiento de 300 por ciento en aproximadamente 1,000 ataques por día vistos en 2015 (fuente: fbi.org How to Protect Your Networks from Ransomware). La Universidad de Calgary fue víctima de un ataque de ransomware en Mayo de 20116. Este ataque daño múltiples sistemas críticos y forzó a la Universidad a pagar $20,000 dólares para poder recuperar acceso a sus sistemas. Una cadena de hospitales en Washington, D.C., fue atacada en Marzo 2016, mientras en Los Ángeles un centro médico pago $17,000 este año a hackers después de un ataque de ransomware. (Fuente: http://bit.ly/2bZF7o2).

Mitos de ransomaware:

Un problema solamente para corporaciones u organizaciones.

Alina Simon escribió un artículo acerca de cómo la computadora de su mama que utilizaba en su casa cayó víctima de un ataque de ransomware en el cual ella se vio forzada a pagar $500 para recuperar su archivos. (Fuente: http://nyti.ms/1xnYhpP). Ransomware es un crimen que se aprovecha en donde aquellos sujetos con malas intenciones tienen como objetivo a cualquier persona que ellos piensan que vayan a pagar el rescate.

Yo utilizo solamente Mac (OS X) y entonces soy inmune al malware.

KeRanger es una variante de ransomware que infecta solamente a OSX. (Fuente: http://bit.ly/2blco7G)

Un gramo de prevención vale un kilo de bitcoins y una cartera más ligera.
Cómo evitar ser víctima de ransomware.

Educación y conciencia: Conocer la amenaza y realizar que si existe. Entender cómo funciona y aprender cómo prevenirla. Compartir el conocimiento con compañeros de trabajo, familia y amigos.

Prevención: Como cualquier malware, actualizar tu computadora regularmente es el método número uno de prevención. Esto incluye tu sistema operativo, tu anti-virus, y otras aplicaciones, especialmente Java, Adobe Reader y tu explorador web. Desinstala cualquier software que no es soportado por el proveedor. (Apple termina suporte para QuickTime en Windows: http://www.utrgv.edu/is/en-us/news-and-alerts/quicktime-eol/)

Buenos habitos en el internet: No hagas click en aquellos links de correos electrónicos de personas sospechosas ni abras documentos adjuntos que tú no esperabas. Instala software solamente de fuentes confiables. ¡Mantente alejado de sitios webs extraños!

Cuando se trata de malware de la computadora, el usuario es el eslabón más débil en la defensa.

Si tiene alguna pregunta o comentario sobre este artículo, por favor envíelos a: is@utrgv.edu

ISO destacó a:

ISO destacó a: es una entrevista de un individuo que juega un rol en la seguridad informática para UTRGV. En este boletín, tú vas a conocer a Thomas Owen, quien es Chief Information Security Officer para UTRGV.

Thomas Owen, CISSP, CRISC, CISA, CISM, CGEIT, C|CISO, CEH, CHFI, MCSA: Security, MCTS, MCITP
Chief Information Security Officer
The University of Texas Rio Grande Valley

Cuéntanos como la seguridad informática ha cambiado desde que empezó en su papel.

Una de las cosas principales es la conciencia. La seguridad informática se está convirtiendo en algo común no sólo en los negocios, pero en la vida personal también. Los individuos son cada vez más conscientes, tienen que proteger su información sensible y ellos también pueden caer víctimas de ataques maliciosos.

¿Quiénes son sus clientes, y cual es una de las áreas más difíciles para usted?

Internamente, mis clientes son estudiantes, maestros y personal de la Universidad. Una de las áreas más difíciles está tratando de encontrar el equilibrio adecuado entre la seguridad y facilidad de uso – queremos establecer el trabajo y aprendizaje pero lo queremos hacer de una manera segura. En esencia, queremos ser un mapa donde puedas llegar fácilmente en lugar de ser un obstáculo en el camino. Encontrar ese equilibrio puede ser difícil dependiendo de los procesos involucrados.

¿Cómo es que llego al campo de seguridad informática?

Crecí en una granja y crecí desde retoques con dispositivos mecánicos a dispositivos electrónicos a dispositivos de red conectados.

Los tres logros mas importantes en su vida

Llegar a ser cristiano
Nacimientos de mis hijos
Matrimonio

La gente se sorprendería saber que:

Puedo hablar gaélico irlandés.

Qué CD tiene usted en su coche? O qué estación de radio te gusta escuchar?

Reckless Kelly – Wicked Twisted Road

Si pudieras entrevistar a una persona (viva o muerta) ¿quién sería?

Jesús

¿Si se les da la oportunidad, que le gustaría ser por un día?

Mi esposa, para poder entender mejor

¿Cuál es el mejor consejo que has recibido y que ha utilizado?

"Aprende a leer un manual. Tu puedes arreglar cualquier cosa." – l abuelo me lo dijo, y ha demostrado ser de un valor inmenso Funciona para cualquier cosa, desde la electrónica a los tractores

¿Cuál sería su consejo para un nuevo profesional en la seguridad informática?

Nunca dejes de aprender. No depende de tu empleador o compañeros de trabajo para que te animes a aprender, lo tienes que hacer por ti mismo para que sea una prioridad. El ámbito de trabajo está cambiando rápidamente, y el conocimiento nunca se pierde.

ARTÍCULOS DE SEGURIDAD INFORMÁTICA

Dropbox- filtración masiva de datos afectando a más de 68M de usuarios

Lo que empezó la semana pasada como una advertencia por Dropbox a sus usuarios que algunos datos pudieron haber sido comprometidos, a explotado en una filtración masiva de datos donde un estimado de 68 millones de credenciales de usuarios utilizando Dropbox fueron expuestas en la web

Las amenazas cibernéticas y Oportunidades—por The University of Texas System Chancellor William H. McRaven

Los ataques cibernéticos se llevan a cabo durante todo el día , todos los días - en las personas, empresas, agencias gubernamentales , los partidos políticos nacionales , lo que sea - y las consecuencias de un solo ataque con éxito pueden ser devastadoras . Esta vulnerabilidad supone una seria amenaza para nuestra economía , nuestro modo de vida , y para nuestra seguridad colectiva.

Ransomware infecto a la Universidad de Calgary

La Universidad de Calgary pagó un rescate $ 20.000 en bitcoins imposibles de rastrear a los hackers después de un devastador ataque de malware. Funcionarios de la universidad aceptaron en pagar el rescate para asegurar que los sistemas críticos podrían ser restaurados , pero señalaron que tomará algún tiempo para que el personal de IT de la universidad para aplicar las claves de cifrado para las máquinas infectadas .

Estos y otros artículos se pueden encontrar en: http://www.utrgv.edu/is/es-es/noticies-y-alertas/index.htm

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

La misión de la Oficina de la Seguridad Informática es proporcionar apoyo a la Universidad en la logro de sus objetivos, garantizando la seguridad, integridad, confidencialidad y disponibilidad de los recursos de información.

1201 W. University Drive
Sugar Road Annex (ESRAX) Building
Edinburg, TX 78539

Phone: (956)665-7823
Fax: (956)665-3154
Email: is@utrgv.edu

Visitanos en la web y en las redes sociales!
www.utrgv.edu/is
www.facebook.com/utrgviso

Servicios que proporcionamos:

CONCIENCIA, RIESGO Y CUMPLIMIENTO

ACTIVOS Y ADMINISTRACIÓN DE LAS VULNERABILIDADES

INGENIERÍA Y RESPUESTA A INCIDENTS

CONCIENCIA, COMUNICACIÓN Y DIFUSIÓN