2013-06-06

Boletín de Noticias de Seguridad Informática # 4

SCProgress

www.scprogress.com

ÍNDICE

NOTICIA 1: Roban información de 9.988 pacientes de clínica de anestesia.

La clínica Presbyterian Anesthesia Associates (PAA) reveló que un atacante tuvo acceso a información personal de 9.988 personas, por medio de una falla de seguridad en su sitio web, de acuerdo con un informe de Charlotte Observer.

Los datos expuestos incluían nombres, información de contacto, fechas de nacimiento y números de tarjetas de crédito. Sin embargo, de acuerdo con la clínica ningún tipo de información médica fue comprometida.

Presbyterian Anesthesia Associates notificó al FBI, que puso en marcha una investigación. La clínica también contrató a Identity Force, una firma de protección de robo de identidad para proporcionar monitoreo gratuito para los afectados.

"Esta información normalmente se descarga con cierta frecuencia y no se mantiene en el sitio web"

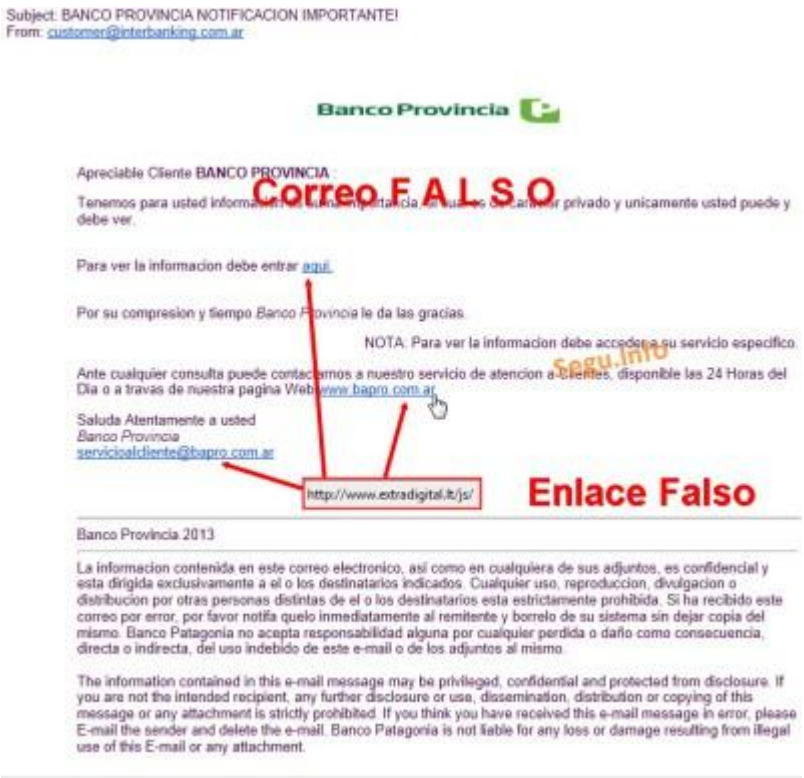
Joseph Ducey, presidente de PAA, dijo a Wsoctv que la empresa E-dreamz donde se encontraba hospedado el sitio, le notificó acerca de la violación el 18 de abril y dijo que se había enterado del incidente el 16 de abril.

Según Ducey, la compañía le dijo que tomó medidas inmediatas para cerrar la brecha. Asimismo, aseguró que la información había quedado expuesta desde el 1 de abril. De igual forma, Ducey comentó que ese tipo de datos de tarjetas de crédito no deberían haber sido almacenados allí.

De acuerdo con el Departamento de Justicia de Carolina del Norte, el robo de datos por violaciones a sistemas se ha vuelto cada vez más común a partir de que las transacciones bancarias se hacen en línea. Más de 1,500 casos que involucran a 4.8 millones de personas en Carolina del Norte se han reportado desde 2005, aseguró el organismo.

Fuente: bSecure

NOTICIA 2: Phishing de Banco Provincia de Buenos Aires

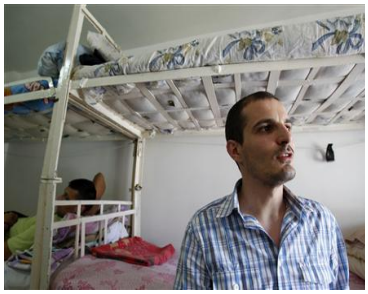


Después de una semana, recibimos hoy una nueva denuncia de correo falso enviado supuestamente por el Banco Provincia de Buenos Aires (Argentina). El (falso) pretexto del mismo se puede leer en el grafico de arriba (errores ortográficos incluidos) que en esa captura se ve el correo y los enlaces que llevaran a la víctima del engaño a un sitio falso.

En los encabezados del correo se observa que el mismo fue enviado mediante una cuenta de correo legítima que ha sido abusada. Los atacantes han conseguido probablemente las credenciales del usuario.

Fuente: segu-info.com

NOTICIA 3: Diseña un sistema contra el Skimming desde la cárcel



El hacker rumano Valentin Boanta, quien cumple una condena de cinco años por estar involucrado en robo de dinero de cajeros automáticos vía skimming, desarrolló desde prisión una tecnología para proteger a los ATMcontra este tipo de ataques. Boanta, de 33 años, fue capturado en 2009 por suministrar a los ladrones con los skimmers que utilizaban para reunir información para clonar tarjetas bancarias y luego robar dinero de los cajeros.

Skimming es el acto de copiar una tarjeta de crédito o débito mediante el escaneo de la banda magnética. Los ladrones luego utilizan estas tarjetas clonadas para retirar dinero de la cuenta bancaria del titular

***"Cuando me atraparon, me puse feliz. Esta liberación me abrió el camino para trabajar por el lado bueno"*, dijo Boanta a Reuters.**

Boanta suministraba, a la banda de delincuentes rumanos, con gadgets que ocultaban cualquier evidencia y que hacían que las tarjetas clonadas lucieran igual a las originales. Su invento, llamado Sistema Rotatorio Seguro (SRS, por sus siglas en inglés) puede prevenir que suceda el skimming. Los usuarios deben insertar su tarjeta en el borde del SRS primero, en lugar del extremo estrecho. De esta manera, cualquier skimmer adjunto u otro gadget de vigilancia no sería capaz de escanear la banda magnética de la tarjeta.

Boanta diseñó el SRS desde su celda en una prisión rumana, que comparte con otros cinco ladrones y una estantería llena de libros y manuales técnicos.

Pero no fue sin ayuda externa: Su investigación estuvo financiada por la empresa rumana MB Telecom, que patentó el SRS.

Aparentemente el dispositivo estará disponible muy pronto, aunque no hay una fecha exacta de lanzamiento.

Mircea Tudor, presidente de MB Telecom, también dijo a Reuters que Boanta definitivamente tendrá trabajo en su empresa cuando salga de la cárcel en cuatro años y medio.

Fuente: www.segu-info.com.ar

NOTICIA 4: **Cronograma de actividades que se llevaran a cabo en el Seminario de Seguridad Informática Perimetral.**

SERVICIOS COMPUTACIONALES PROGRESS

SISTEMAS DE SEGURIDAD INFORMATICA INTELIGENTE

AGENDA DEL SEMINARIO GESTION UNIFICADA CONTRA AMENAZAS INFORMATICAS

08:30 – 09:00	Registro
09:00 – 09:10	Introducción
09:10 - 09:35	Conceptos básicos de seguridad y networking
09:35 - 10:00	Cyberoam Identity Based UTM
10:00 – 10:20	Información general sobre productos marca Cyberoam
10:20 – 10:30	Preguntas y premios
10:30 – 10:50	Coffe Break
10:50 – 11:10	Cyberoam despliegue en la red.
11:10 – 11:35	Firewall
11:35 – 12:00	Formas de autentificación de los usuarios.
12:00 – 12:25	Diferentes alternativas para el filtrado de contenidos.
12:25 – 12:40	Alternativa para minimizar el riesgo informático , Application filter
12:40 – 12:50	Gateway Anti-Virus / Anti-Spam
12:50 – 13:00	Preguntas, respuestas y premios

13:00 - 13:50	Almuerzo Buffet
13:50 – 14:10	Sistema Detector de Intrusos y Prevención (IDS & IPS)
14:10 - 14:30	Virtual Private Network (VPN)
14:30 – 14:55	Gestión de enlaces redundantes (Multilink Manager)
14:55 – 15:20	Routing & QoS
15:20 – 15:45	Administración general y reportes
15:45 – 16:00	Preguntas, respuestas y premios
16:00 - 16:20	Coffe Break
16:20 – 16:40	Preguntas, respuestas.
16:40 - 16:55	Sorteo del premio mayor entre los participantes del seminario
17:00	Clausura del evento