Seguridad Informática

Ediciones Especiales

ALTAS PROYECCIONES FUTURAS

Seguridad informática es un deber en el aula, las empresas y el hogar

Cada día más instituciones incorporan herramientas computacionales en sus procesos, lo cual ha derivado en una mayor demanda de profesionales especializados en prevenir ciber ataques. Las universidades e institutos con carreras del área han sumado estas materias en sus mallas curriculares con el fin de evitar amenazas a nivel de hardware, software y redes.

Ni los expertos más visionarios podrían haber anticipado la relevancia que las tecnologías digitales tienen en la vida cotidiana de cientos de millones de personas. Ya no se trata sólo de computadores, la informática se está apoderando de todo; desde la manera en que nos comunicamos y trabajamos hasta controlar los artefactos del hogar desde cualquier punto del planeta. Lamentablemente, aquel desarrollo no está exento de riesgos y malas prácticas que parecen aumentar cada día.

Allí el concepto de seguridad informática surge con fuerza, abarcando centros de investigación y una creciente presencia en la malla de universidades e institutos profesionales, en especial en carreras informáticas y del ámbito técnico en general.

La mayor oferta académica ha ido de la mano con las necesidades urgentes de clientes de todo tipo. Hemos visto como los hackeos a cuentas personales pueden destruir vidas, pero también existen diversas amenazas a empresas y corporaciones que hoy ya cuentan con un servicio de protección a cargo de profesionales. Sin embargo, ese es un aspecto en el que todavía nos queda bastante por avanzar.

Según explicó Patricio Galdames, académico de la UBB y doctor en Ciencias de la Computación de la Iowa State University of Science and Technology, "el principal problema parte desde la misma organización o empresa. Deben reconocer que este no es un gasto, sino una inversión que tienen que hacer para efecto de mantener su negocio y conservar su reputación. Un ejemplo reciente fue el del Banco de Chile, donde todavía se aprecian las implicancias que el ataque tuvo en el servicio a sus clientes, algunos de los cuales cerraron sus cuentas para evitar problemas", explicó.

Pero no sólo las grandes empresas deben poner atención a los ataques informáticos. Toda institución que maneje redes, correos electrónico e incluso sistemas de producción automatizados están en riesgo. "Se han dado casos de todo tipo en la Región, y es que falta considerar esto como un gran tema. Con el ramsonware del año pasado se dio un impacto bastante fuerte y recuerdo casos de afectados en Chillán y en Coronel. Muchos piensan que estas cosas suceden en las películas, o sólo en Estados Unidos y en Europa; pero cada vez la internet penetra más en nuestras actividades, y estos fenómenos no deseados están llegando con una fuerza preocupante", enfatizó el experto.

Desde distintos ángulos

Ante la cantidad de áreas y situaciones que involucra la seguridad informática, es importante diferenciar los distintos tipos de riesgos, los que han sido clasificados en tres categorías. La primera es la seguridad del hardware; la cual se relaciona con un dispositivo que se utiliza para escanear un sistema o controlar el tráfico de red. Los ejemplos más comunes incluyen cortafuegos o firewalls de hardware y servidores proxy. Otros ejemplos menos comunes incluyen módulos de seguridad de hardware (HSM), los que suministran claves para funciones críticas tales como el cifrado, descifrado y autenticación para varios sistemas. También se refiere a cómo podemos proteger nuestros equipos físicos de cualquier daño, incluyendo dispositivos como tablets, teléfonos celulares y smart tv.

200

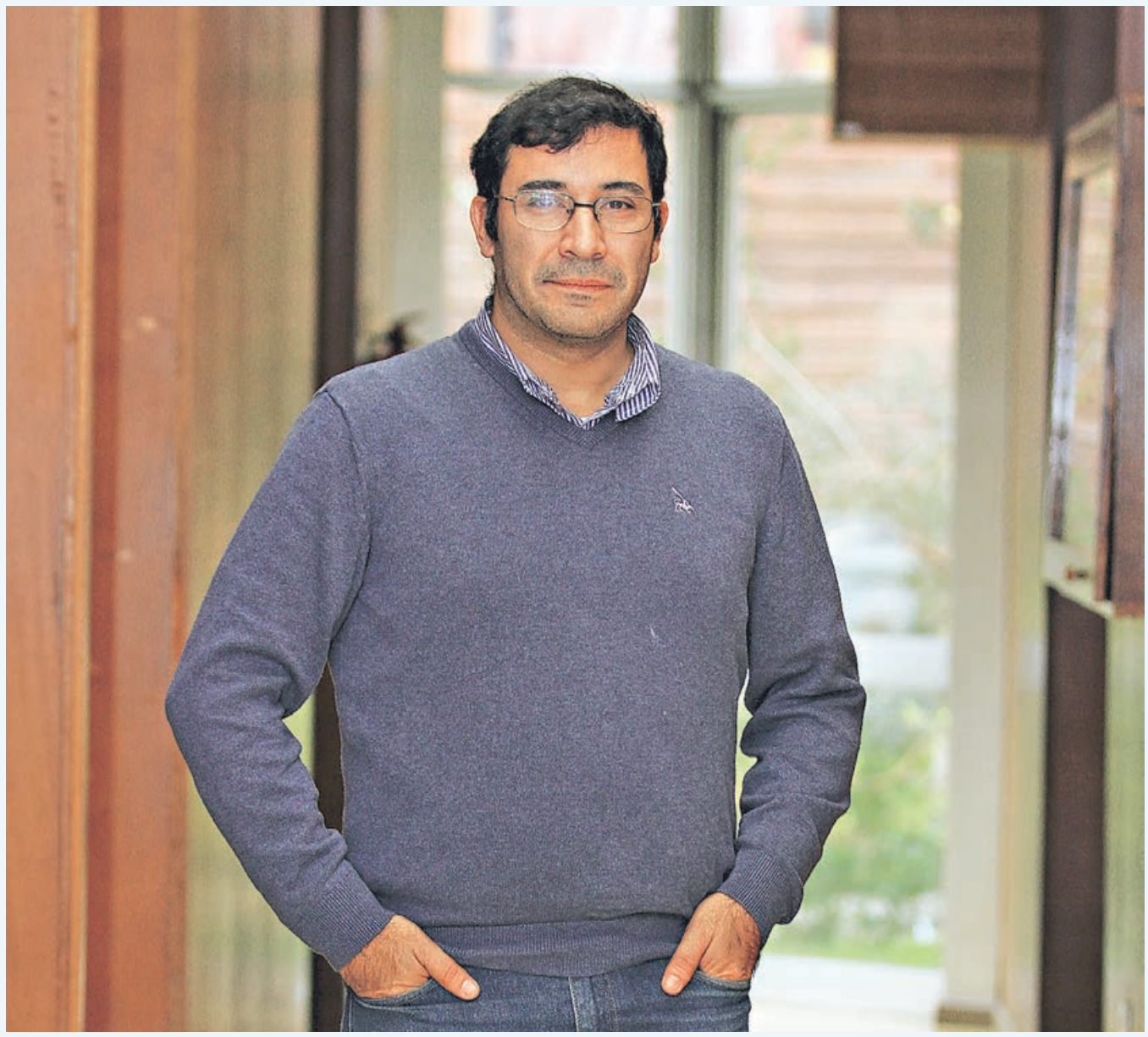
billones de mails con categoría de spam o malware se enviaron cada mes durante el año pasado, según Microsoft. En Chile, se estiman 14 mil ataques de diversa índole por segundo

Una segunda línea es la seguridad del software. Allí el objetivo es protegerlo contra ataques maliciosos de hackers y otros riesgos. Es necesaria para proporcionar integridad, autenticación y disponibilidad. Entre los problemas a solucionar están los errores de implementación, desbordamientos de buffer, defectos de diseño, o mal manejo de errores; los cuales están entre los más comunes debido a la proliferación de intrusos maliciosos.

A lo anterior se suma la seguridad de red. Estas actividades protegen la facilidad de uso, fiabilidad, integridad y seguridad de su red y datos; implicando una variedad de amenazas como virus, gusanos y caballos de Troya; así como softwares espías y publicitarios, ataques de hackers, intercepción o robo de datos o denegación de servicios.

Ante este escenario se recomienda no confiar en un sólo sistema de protección, sino incluir varios niveles de seguridad que operen como respaldo. Entre las opciones hoy encontramos cortafuegos para bloquear el acceso no autorizado a su red; sistemas de prevención de intrusiones (IPS), para identificar las amenazas de rápida propagación; y redes privadas virtuales (VPN), para proporcionar acceso remoto seguro; entre otras medidas de seguridad.

Edición Especial **Seguridad Informática**



HAY BUENAS PERSPECTIVAS LABORALES

UBB asume el liderazgo en el área académica e investigación aplicada

El plantel penquista ha sumado la especialización en ciberseguridad como parte de sus carreras de ingeniería informática. A ello se suman alianzas con otros planteles, investigaciones aplicadas, laboratorios, y el desarrollo de aplicaciones vinculadas a la gestión de privacidad.

Considerando el papel que la informática cumple tanto en las empresas como en la vida cotidiana, la Universidad del Bío Bío ha sabido incorporar distintas materias ligadas a la seguridad en sus distintas carreras del área, comenzando con los casos de Ingeniería Civil Informática e Ingeniería en Ejecución en Computación e Informática. Además, en los últimos años ha destacado en ámbitos como el desarrollo de programas e investigación aplicada.

Según explicó el académico del Departamento de Sistemas de Información, Patricio Galdames, "esta opción ha ido creciendo en la medida que se está tomando una mayor conciencia de los riesgos y consecuencias de los ataques cibernéticos; siendo un campo que además requiere de constante actualización", enfatizó. Bajo esa premisa, la UBB se ha mantenido a la vanguardia en la enseñanza de esos procedimientos específicos.

"En el caso del pregrado, hoy estamos con un curso que da un barniz general del tema; con distintos modelos que permitan al alumno detectar cuales son los límites de acción; pues no todos los problemas son solucionables por cuenta propia. También abarcamos ciertos aspectos de los principales problemas de seguridad en sistemas autónomos operativos, con sus principales vulnerabilidades; así como distintas modalidades para la detección de hackers", explicó el ingeniero y Doctor en Ciencias de la Computación de la Universidad de Iowa.

"También vemos redes y tipos de ataques, con análisis de casos y aplicación de herramientas de defensa. Otro aspecto de gran relevancia es el tema ético, con debates entre los alumnos; así como el conocimiento de la legislación local; la cual igual funciona en algunos casos y se está aplicando de a poco, como ha sucedido con hackers chilenos encarcelados por delitos informáticos. Aun así, tenemos mucho que avanzar en esa materia.

Liderazgo en la Región

El tema de la seguridad informática dentro de las carreras del área en la UBB comenzó a tomar fuerza hace una década con el proceso de acreditación del plantel, lo que motivó la incorporando de especialistas. Fue entonces cuando Patricio Galdames su sumó a través de un concurso académico. "Una de las primeras tareas en que me tocó emprender fue el crear una asignatura para el pregrado con el objetivo de abarcar materias de seguridad que hasta entonces no se incluían en la malla", comentó el docente.

"Se optó por que este fuera un curso del último año, pues una de las características de la seguridad informática es que requiere conocimientos integradores de múltiples disciplinas, y que también están en el programa, como es el caso de base de datos, sistemas operativos e ingeniería de software, por mencionar algunos".

Galdames agregó que en el último tiempo además se implementaron laboratorios para que los alumnos apliquen conocimientos teóricos sobre el tema y maduren esos conceptos. "He ido incorporando apoyos técnicos y existe un interés creciente entre los alumnos ante las perspectivas laborales que ofrece. Se ha planteado ir sumando otras carreras, y es probable que así sea en el futuro".

El renombre que la UBB ha ido alcanzando en el área de la ciberseguridad además se potencia gracias a la interacción con profesionales de las universidades de Talca y de la Frontera, en Temuco; como parte del proyecto de Ingeniería 2030, alianza que busca fortalecer a las facultades de Ingeniería involucradas, generando una macro-facultad con estándares de calidad compartidos y de nivel internacional.

El trabajo está enfocado en formar especialistas en Seguridad Informática, la cual cubre muchos temas. Se ha asumido que en la UBB tengamos el liderazgo en la zona, por lo que cada año surgen nuevos proyectos e investigaciones.

> "A veces, como usuarios, aceptamos cualquier aplicación y no estamos conscientes de los detalles de instalación o de la letra chica, lo que quizás permitirá enviar la ubicación de tu teléfono. Allí queda un desafío para los informáticos, pues se pueden desarrollar otras herramientas que sean más evidentes y menos invasivas"
>
> **Patricio Galdames**
> **Académico UBB**

Expertos de alto nivel

Claro está que el camino a la experticia no es fácil. "A los alumnos se les enseña, desde un principio, que existen ciertos elementos básicos como los antivirus o a mantener actualizado el sistema operativo. Acá, como hay que desarrollar sistemas, deben saber que en la industria hay buenas prácticas de cómo se hace desarrollo seguro de softwares, y hacer un buen uso de las herramientas con que cuentan. Deben reconocer posibles amenazas para la integridad del sistema, pero también la red en la cual está ese equipo", contó el académico.

"En el mundo de la ciberseguridad hay mucha jerga y se debe conocer bien dónde se va a publicar la información más actualizada. Es que esta es una carrera contra el tiempo, muchas veces los problemas surgen antes de que uno se entere y es importante tener investigaciones recientes a la mano para saber cómo proceder ante cualquier alerta. Por otra parte, hay todo un rol de prevención; es como una enfermedad. No siempre se reconocen los síntomas, y lo más conveniente es asistir a control con regularidad".

Gestión de privacidad

Considerando las actuales tendencias y comportamientos en el uso de las nuevas tecnologías, la UBB ha ido a la par con la contingencia, aplicando investigación y desarrollo en el tema de la privacidad; un derecho que está siempre en la palestra, ya sea por casos personales como por estrategias corporativas que muchos desconocen.

"Es el gran tema de hoy. Se está dando a nivel mundial y acá en Chile estamos en pañales, pues no somos conscientes de la información que se está liberando. Hay casos que incluso llegan a niveles macropolíticos como el de Donald Trump y la injerencia rusa en tiempo de elecciones" alertó el académico Patricio Galdames.

"Por otra parte, el marketing está individualizando a los clientes, y eso tiene aristas tanto positivas como negativas. Es importante saber para qué se están usando mis datos y si se contó con mi aprobación".

En cuanto al aporte de la UBB a este tema, el académico sostuvo que actualmente un equipo de académicos está trabajando en una línea directamente relacionada a la seguridad informática y el derecho a la privacidad. "Algunos trabajos recién publicados se refieren a cómo acceder a servicios que requieren de la ubicación del usuario y cómo puedo proceder protegiendo mi posición. Por ejemplo, se han dado casos de esposos despechados que usan esa opción para espiar a la ex señora. La ubicación es un tema muy actual, con aplicaciones buenas como Waze pero también está abierto a usos maliciosos e incluso peligrosos", enfatizó Patricio Galdames.

Edición Especial Seguridad Informática

UN TEMA MUY INTERESANTE

Desde una infidelidad hasta un ataque nuclear

Los contenidos mediáticos han generado un creciente interés por el tema de la seguridad informática, ya sea en las noticias o en series documentales disponibles en la plataforma Netflix. Entre los recomendados destaca el seguimiento a la vida de John McAfee, una serie con el lado oscuro de la web, el hackeo al portal Ashley Madison, y las amenazas que la informática ofrece al espionaje y el terrorismo.

Todos quienes tienen un computador o un celular pueden ser víctimas de un ataque cibernético o de otras prácticas maliciosas. Ello es tan evidente que todos los días vemos noticias sobre el tema. Es más, recién esta semana se dieron casos como un hackeo interno en un banco para robar millonarias sumas o la prohibición de uso de celulares en reuniones de gobierno ante la posibilidad de ciber ataques advertidos por el Ministerio de Defensa.

Al tratarse de un asunto con muchas aristas y variedad de consecuencias, los medios han estado abarcando la temática en reportajes y documentales. Actualmente, la conocida plataforma Netflix cuenta con varias producciones que hablan del tema; desde el seguimiento a la peligrosa vida del excéntrico informático John McAfee creador del famoso antivirus; hasta la serie "Dark net" que explora el lado más oscuro de la internet, incluyendo el modus operandi de mafias criminales, los resquemores ante la inteligencia artificial o el modo en que operan los círculos de pedofilia. Los engaños con perfiles falsos en redes sociales también afloran en la serie, con desenlaces bastante más serios que los vistos en programas más livianos como "Catfish, mentiras en la red" de MTV, el cual incluso tiene versiones por toda Latinoamérica, incluyendo Chile.

La batalla contra el ciber crimen parte por casa

En la mayoría de los reportajes sobre el tema se insiste en medidas como cambiar de contraseña, no revelar datos personales, usar antivirus, evitar programas piratas, no acceder a páginas sospechosas, etc.

Riesgos planetarios

Un título interesante es "Sex, lies and ciberatacks" el cual muestra el caso del portal de citas Ashley Madison, dedicado a personas que desean ser infieles y que a poco andar ya tenía ganancias multimillonarias. El golpe lo dio un grupo de hackers llamado Team Impact, el cual amenazó publicar el listado de usuarios, así como cuentas personales y correos electrónicos a menos que bajaran la página. Al no acceder, los hackers cumplieron con la advertencia y el resultado fue incluso más allá de las familias destruidas. Se descubrió una red internacional de prostitución y hasta hubo suicidios como consecuencia.

Armas en potencia

Sin embargo, el título más atractivo e inquietante disponible en Netflix es "Amenaza de ciberguerra". Allí se muestran las prácticas de la Agencia de Seguridad Nacional de Estados Unidos, interviniendo y accediendo a información privilegiada; lo cual hoy muchos ya conocen tras el caso Snowden. Entre los puntos preocupantes está el espionaje entre países, así como el interés de grupos terroristas por desarrollar estas alternativas para fines destructivos.

"Cada computador es un arma en potencia" es la sentencia que parece guiar al documental. Y es que los peligros de las nuevas tecnologías parecen tener tantas ventajas como riesgos. Un hacker podría intervenir un sistema de control de trenes o de aviones, abrir escotillas de un suministro de agua potable o sabotear una misión espacial.

Puede parecer exagerado, pero en el film se muestra el caso del ciberataque a la planta nuclear en Natanz en Irán. El fenómeno se repitió cinco meses después, pero esta vez los expertos pudieron detectar la causa: un malicioso virus informático.

El "gusano", ahora conocido como Stuxnet, tomó el control de mil máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse, un caso digno de una película James Bond.