

Seguridad Informática en las empresas

Hernán Alberti

www.carranzatorres.com.ar

Los parches cubren los vacíos que el tiempo se encarga de destapar nuevamente. Son instrumentos que sirven para dar continuidad a cualquier andamiaje. Y funcionan. Tal vez, ningún término lo defina mejor: funcionan. Ahora bien, en tren de escuchar los motores en marcha ¿Podemos pensar a la seguridad informática de las empresas, en muchos casos, como una sucesión de parches por el sólo hecho de funcionar? La respuesta se derrumba sola: no.

Algunos estudios, publicados recientemente, se han encargado de demostrar que las organizaciones sólo cumplen con los requisitos mínimos de protección que rigen el mercado. A pesar de las denodadas advertencias para que regulen el uso interno del correo electrónico o que prevengan sus zafiros más preciados como lo secretos comerciales, datos confidenciales o la pérdida de información, la seguridad corporativa sigue siendo un tema ignorado en las agendas empresariales y, por el momento, una dilema en los ámbitos legislativos por la ausencia de leyes más rigurosas y específicas.

Ser parte

La seguridad pareciera ser un simulacro de protección para espantar reformas estructurales. Si bien es cierto que durante el 2005 hubo mayores inversiones en pos de montar líneas de protección, las empresas sólo procuraron cumplir con las normas que establecen los mercados para no ser sancionadas. Sólo el 41% aprovechó esa oportunidad para diseñar un cambio de cimientos en sus sistemas y prevenir los diversos problemas que pueden descolgarse del ciberespacio como robo de datos o fraudes informáticos. Según informes de diversas consultoras, durante el 2006 el 60 % de las compañías continuarán ajustadas al parquímetro de las regulaciones y tan sólo un tercio le dará importancia a los gusanos y virus, contra más del 50% registrado el año pasado.

Las normas son para cumplirlas, vaya precepto. Pero las organizaciones no deberían actuar persiguiendo a las leyes si no dentro de las leyes. Porque, aunque insuficientes, sirven como referencias para construir un nuevo marco legislativo que logre monitorear la seguridad informática y aporte tranquilidad al sector empresarial. Es decir, aprender sobre lo llovido. Para que la ley, en mayor o menor medida, la jurisprudencia, los casos y experiencias de otras compañías puedan y sean utilizados para poder detectar y frenar ataques informáticos dentro una compañía.

Un buen antídoto

Para prevenir es necesario conocer el campo. Y como las hectáreas del mundo tecnológico resultan inalcanzables es mejor poner freno para no andar deambulando sin destino cierto y no toparse con sorpresas que puedan hacer perder el trabajo de años. La seguridad informática no es sólo una carrera por quien invierte más o menos recursos en sus arcas corporativas. Debería ser un estado de conciencia que llevara a las empresas a determinar que la protección es un fin y no un medio para cumplimentar con la normativa vigente.

Es bueno recordar que la mayor inversión no es la única variable para disminuir los ataques, ni garantiza inmunidad. También es preciso que se estipule una sostenida capacitación de los empleados, una disuasiva y preventiva política de seguridad y un manual de uso de herramientas informáticas ante posibles

desastres, que entre otras cláusulas incluya: normas de integridad de datos, de confidencialidad de la información y de control de acceso, entre otras medidas.

Prevenir y planificar un registro de las operaciones corporativas son, hasta el momento las mejores herramientas para evitar posteriores litigios. Según estudios realizados recientemente más del 60% de las firmas aplicó controles internos durante el 2005. Ese porcentaje se incrementará un cinco por ciento durante este año.

Si las empresas no logran anticipar y proteger sus recursos con pautas claras, intentarán nuevamente tapar los desastres con parches. Y los parches ya sabemos, sirven para que los andamiajes funcionen un tiempo, pero que no duren para siempre.