

# ¿Piensa usted como un Hacker? Nosotros sí.

*"Indiscutiblemente, las Nuevas Tecnologías nos han facilitado mucho el trabajo, pero debemos ser conscientes del riesgo que comporta tener toda la información almacenada en un equipo informático."*

Con estas palabras comienzan Daniel Fernández y Vicente Aguilera la entrevista mantenida con nosotros acerca del valor de la seguridad telemática, sobre todo para las empresas. Ambos son socios fundadores de Internet Security Auditors, una compañía dedicada exclusivamente a ofrecer servicios de seguridad informática, que cuenta con especialistas en diferentes áreas tecnológicas, los cuales han dirigido sus conocimientos hacia un enfoque común: el Hacking Ético. La especialización de la compañía en servicios de seguridad, la utilización de metodologías reconocidas mundialmente, la experiencia y conocimiento de sus técnicos y el continuo proceso de estudio e investigación, le permiten ofrecer a sus clientes servicios de calidad y acordes a sus necesidades.

## Los servicios que ofrece

### Internet Security Auditors:

- Test de Intrusión.
- Auditorías de la DMZ y Red Interna.
- Consultoría de Seguridad.
- Seguridad para PYMES.
- Adaptación y Auditoría de LOPD/LSSICE
- Auditoría de Aplicaciones.
- Formación.
- Seguridad en redes Wireless y VPNs.

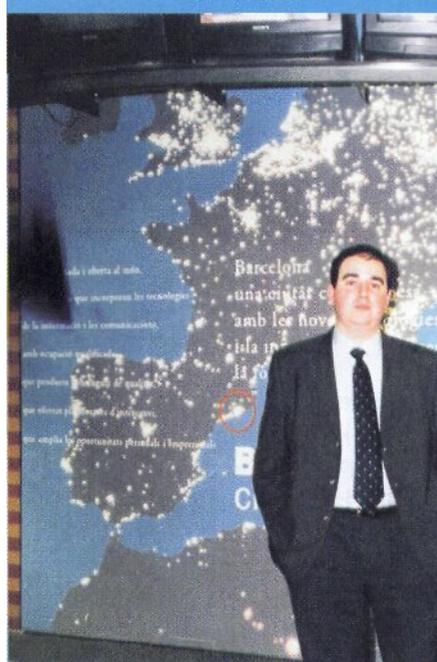
Hoy día existen una gran cantidad de empresas que utilizan Internet en su cadena de valor. Sin embargo, la gran mayoría de ellas no se han concienciado aún de los peligros que este hecho comporta, "en parte por pensar que un hacker tiene un objetivo definido y sólo ataca a las grandes compañías, y en parte por relacionar los servicios de seguridad con elevados costes para la empresa", comenta Vicente Aguilera. "Sin embargo -continúa- toda empresa necesita seguridad. Existen estadísticas que demuestran que el 70% de los hackers toman su víctima de manera aleatoria, sin saber siquiera a qué empresa están atacando, por no hablar de los virus y los gusanos, que se propagan rápidamente a través del correo electrónico." "Además -añade Daniel Fernández- la rentabilidad de la inversión realizada en seguridad es inmediata, pues ataques como robos de información confidencial, caídas de los sistemas, etc. causan pérdidas mucho mayores al coste de una seguridad previamente planificada."

Sin duda, hay algo de cierto en el hecho de pensar que la seguridad implicaba un considerable desembolso económico, pero eso era hace algunos años, cuando aún no existían empresas independientes y especializadas en estos temas, capaces de entender las necesidades de cada cliente y consecuentemente aplicar las medidas que más se ajustan a la situación.

El planteamiento de Internet Security Auditors es el de detectar los problemas de seguridad de las empresas empleando las mismas técnicas que los hackers, junto al rigor que aporta el uso de metodologías abiertas y estándares de seguridad. Pero su objetivo principal es el de ofrecer a sus clientes soluciones a estas deficiencias de seguridad a través de sus servicios de auditoría, consultoría e implantación de sistemas. Como complemento a estas soluciones, Internet Security Auditors, imparte cursos de formación específicos en seguridad.

"Es tan importante implantar un sistema de seguridad como revisarlo", apunta Daniel. "La tecnología cambia, aparecen nuevas vulnerabilidades que se deben controlar. La seguridad es una labor permanente. Es importante emplear metodologías de trabajo que se adapten a las nuevas tecnologías, como las redes wireless o las VPN's." "Las PYMES pueden contar con el apoyo de grandes profesionales (y en nuestro país los hay) capaces de aportarles soluciones globales y asequibles. Lo importante es que se mentalicen de la trascendencia de la seguridad, pues el índice de atacantes y ataques potenciales es cada vez mayor. Desgraciadamente, el número de los que juegan a ser hackers crece a un ritmo vertiginoso", concluye Vicente.

PILAR MORATE



Daniel Fernández y  
Vicente Aguilera

## Los consejos de los profesionales

- Actualizar y securizar los sistemas y aplicaciones informáticas.
- Contar con una política de seguridad.
- Formar a los usuarios: los virus informáticos que se propagan vía e-mail son demasiado frecuentes.
- Contar con la visión externa y objetiva de expertos en seguridad.
- Evaluar y controlar periódicamente la seguridad.



**INTERNET SECURITY AUDITORS, S.L.**  
C/ Llacuna, 162 - 08018 Barcelona  
Tel. y Fax: 93 401 96 97  
info@isecauditors.com  
www.isecauditors.com