

Combate eficaz à fuga de informação

A fuga de informação corporativa é actualmente uma das grandes preocupações de qualquer organização. O aumento do número de incidentes com grau de sofisticação e impacto na segurança é cada vez maior, o que obriga as empresas a disporem de sistemas de gestão e de controlos de acesso à informação cada vez mais eficazes para minimizar o impacto deste tipo de ocorrências.

Actualmente, existe uma grande diversidade de dispositivos e sistemas de protecção alinhados com as necessidades de cada tipo de negócio e que oferecem às organizações uma plataforma de gestão operativa de segurança, além de especialistas em segurança informática que se responsabilizam de forma operativa pela protecção dos sistemas informáticos. Firewalls, antivírus, encriptação e certificados são palavras amplamente conhecidas quando se trata da protecção dos sistemas informáticos. Porém, a segurança inclui também riscos, normas, pessoas, processos e organização num ambiente cada vez mais complexo, variável e exigente.

Uma forma de combater a fuga de informação passa por auditar a segurança da organização ao nível dos sistemas,

aplicações e infra-estruturas, com o objectivo de analisar e dar a conhecer às empresas o seu grau de cumprimento e de exposição ao risco e propor medidas de correcção.

Adicionalmente, o investimento num Serviço de Gestão da Segurança (Managed Service) oferece às organizações o conhecimento exacto sobre o seu estado actual e evolução da segurança. Estes serviços permitem que a segurança deixe de depender da sorte ou da intuição, para se basear em critérios exactos. Através destes serviços, as organizações aumentam proactivamente a capacidade de identificar vulnerabilidades e mitigar riscos, o que permite incrementar o conhecimento que têm sobre o impacto real dos incidentes para o negócio.

Ainda assim, conhecer não é suficiente, uma vez que, com o tempo, são efectuadas mudanças, surgem novas vulnerabilidades ou ocorrem incidentes e o que antes não era importante pode passar a sê-lo. É essencial gerir e implementar o que for necessário para que o programa de segurança se antecipe, reaja e evolua face às mudanças da organização e do ambiente. É fundamental conhecer e controlar to-



dos os pontos de acesso, criar um sistema capaz de evoluir da mesma forma que a organização e melhorar em simultâneo os factores de cumprimento, risco e custos. É necessário implementar a segurança como um processo, com entradas, saídas, indicadores e mecanismos de controlo, permitindo um ciclo contínuo de melhoria através de um Sistema de Gestão de Segurança da Informação (SGSI). Mas, para garantir o sucesso da gestão de segurança da informação, é fundamental a qualidade de uma metodologia apurada, a

certificação (CISSP, CISM, CISA, CEH) das capacidades dos recursos humanos e o conhecimento adquirido após numerosos projectos.

Em suma, a segurança não deve ser vista como mais um projecto, mas sim como um processo contínuo em melhoria constante, alinhado com a TI/SI e com o negócio, de forma a aumentar a segurança mas também a produtividade da organização.