

Como proteger os dados de uma empresa?

Quais as três medidas que uma empresa nunca deve deixar de tomar relativamente à segurança dos seus dados?

Fomos ao mercado procurar respostas.

E apesar de todas elas explicarem que essas medidas podem variar, dependendo da realidade da empresa, de uma forma genérica acreditam que as três sugestões que deram são transversais a todas as estruturas.

SUSANA MARVÃO
s.marvao@vidaeconomica.pt



- ✓ Conhecer o estado actual do nível de Segurança do IT da Organização (Security Assessment)
- ✓ Definir as normas de Segurança da Organização (Security Governance)
- ✓ Construir uma infra-estrutura de Segurança que enderece as debilidades do IT (Trustworthy Infrastructure) e designar e formar os colaboradores internos com competências na área de Segurança ou recorrer a parceiros que possam preencher eventuais carências (Managed Security)

SYBASE

- ✓ Mobilizar apenas a informação necessária, ou seja, controlar o processo de mobilização dos dados.
- ✓ Assegurar a segurança da informação mobilizada.
- ✓ Gerir os dispositivos dos colaboradores de uma forma eficiente.



- ✓ A primeira medida passa pela existência de uma sólida infra-estrutura de segurança (contendo firewall, antivírus, patch management, SIEM, etc), possibilitando ter mecanismos de defesa contra potenciais ataques.
- ✓ A segunda medida é a criação de uma política, normas e procedimentos de segurança.
- ✓ Por fim, deverá ser garantido que, pelo menos anualmente, é realizada uma auditoria de segurança, tendo como objectivo tirar uma "foto" da organização para observar como está a empresa em relação à temática da segurança, se tem muitas vulnerabilidades e como mitigá-las.



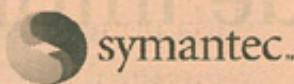
- ✓ Instalação de uma firewall na rede, que seja instalada e administrada por um técnico especializado. A firewall deve ser actualizada constantemente tal como um programa de segurança, senão torna-se rapidamente ineficaz e vulnerável.
- ✓ Instalar uma solução de segurança completa que englobe antivírus, anti-spyware, anti-spam, anti-rootkit, etc. e que possua uma administração centralizada.
- ✓ Realizar cópias de segurança regularmente e guardá-las num lugar seguro e protegido.



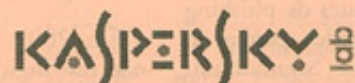
- ✓ Implementação de sistema de backups de segurança da informação vital adequado à realidade da empresa;
- ✓ Implementação de sistema de segurança contra agentes externos, recorrendo por exemplo a firewalls e antivírus, adequada à realidade da empresa;
- ✓ Implementação de regras de segurança internas que permitam quer o controlo de acesso a informação vital quer a salvaguarda dessa mesma informação.



- ✓ A primeira é, sem dúvida, uma firewall. Depois a implementação de gestão de acessos e políticas de mudança de passwords, já que muitos utilizadores utilizam sempre a mesma ou até a que lhes foi atribuída inicialmente.
- ✓ Outra das medidas que recomendamos é um sistema de base de dados seguro, que garanta a fiabilidade dos dados e com uma política de backups, razão por que baseamos o software PHC na base de dados SQL cuja estabilidade e integridade é reconhecida.



- ✓ Implementar estratégias de defesa profundas, que enfatizam sistemas de defesa múltiplos, que se sobrepõem e que se apoiam mutuamente de forma a proteger contra falhas de apenas um ponto único numa tecnologia específica ou método de protecção. Deve-se incluir a instalação de antivírus, firewalls, detecção de intrusos regularmente actualizada, como também de sistemas de protecção contra intrusos nos sistemas de clientes e controlo de dispositivos e acessos às redes de dados (NAC - Network Access Control).
- ✓ Educar/formar os colaboradores na correcta utilização dos seus sistemas e aplicações, de modo a torná-los numa segurança pro-activa e reactiva, que nenhum mecanismo tecnológico consegue equiparar-se e que pode passar por simples procedimentos, como: não abrir ficheiros de anexos, a não ser que esteja à espera dos mesmos e que estes venham de uma fonte de confiança, não executar software que derive de um download através de Internet, a não ser que este tenha sido monitorizado em relação à presença de vírus, etc.
- ✓ Assegurar que os procedimentos de resposta em caso de emergência estão correctamente implementados. Isto inclui a existência de uma solução de backup e recuperação, de forma a recuperar qualquer sistema ou informação perdida ou comprometida na eventualidade de um ataque bem sucedido ou uma catástrofe de perda de dados.



- ✓ Proteger o acesso de entrada na empresa (com firewall e sistemas de VPN);
- ✓ Garantir que todos os terminais, ao acederem aos serviços da Internet, passam por servidores de comunicação em modo Proxy, garantindo que o utilizador nunca se liga directamente à Internet e portanto a servidores potencialmente perigosos (armadilhas para incautos);
- ✓ proteger todos os terminais com software de antivírus com tempos de actualização curtos, taxas de detecção altas, evitando que, se os conteúdos forem infectados pelos servidores, em pouco tempo possam vir a ser eliminados dos terminais.



- ✓ É importante que uma empresa aposte na formação dos seus utilizadores, em matéria de segurança, e tudo começa pelo simples facto de a grande maioria das empresas não ter a noção exacta da importância da informação que processa. Parece evidente que a melhor protecção é estar alerta, conhecer os riscos e partilhar essa informação com as pessoas indicadas. Os passos na Internet devem ser dados com muito cuidado e de forma sustentada. É verdade que a Internet abre uma porta para o mundo mas também o conduz na nossa direcção, resta-nos avaliar bem o que vem na nossa direcção. E nunca é de mais referir que é imprescindível proteger os sistemas empresariais com um antivírus, anti-spyware, anti-spam e firewall, de forma a controlar a entrada e a saída de dados das máquinas.

FORMAÇÃO DOS UTILIZADORES TEM PAPEL PRIMORDIAL

Antivírus, anti-spyware, anti-spam, firewall... Estas são apenas algumas das ferramentas que as empresas não podem, não devem e de certeza que não querem deixar de ter por perto quando falamos em segurança dos sistemas de informação. Mas a verdade é que essa mesma segurança extravasa em muito este tipo de aplicações. O comportamento dos utilizadores face aos meios de que dispõem nas empresas é a primeira forma de prevenir falhas na segurança dos sistemas. Para isso, a aposta na formação dos utilizadores parece ser ponto consensual entre as empresas convidadas a dar sua opinião. Há mesmo empresas que já nem sequer falam em formação. Antes, falam em educação. Porque muitas vezes não deixa quase de ser quase um problema cultural. Como o simples caso de deixarmos as passwords facilmente acessíveis a quem visita o nosso posto de trabalho. Renato Lopes, account manager mid-market da McAfee para Portugal, mencionou uma curiosa frase: "É verdade que a Internet abre uma porta para o mundo mas também o conduz na nossa direcção, resta-nos avaliar bem o que vem na nossa direcção."