ZURICH

Proteção de dados e *software de computador*

Proteção de dados e software de computador

Introdução

Com a dependência comercial dos sistemas de computadores, a questão da proteção aos dados e software do computador é de suma importância em relação aos aspectos físicos, como danos causados por fogo, calor e água. Além disso, é preciso ter cuidado para se proteger contra o risco potencial de corrupção e / ou manipulação de dados e software, cujas consequências podem ter uma influência significativa na eficiência diária de uma empresa. Mais recentemente, a proteção dos dados pessoais de clientes e funcionários tornou-se cada vez mais importante com desenvolvimentos como a Lei de Proteção de Dados de 1984 e a Lei de Proteção de Dados muito mais ampla de 1998 e o aumento significativo de roubo de identidade, fraude e atividades criminosas semelhantes.

Os dados e o software do computador devem ser protegidos em um grau apropriado à sua importância. A vigilância da equipe e a conformidade com uma estratégia de segurança de dados são vitais para alcançar níveis adequados de proteção. Para conseguir isso, a gerência deve nomear pessoas responsáveis pela manutenção dessa estratégia.

As diretrizes a seguir foram projetadas para auxiliar no fornecimento e manutenção de precauções de segurança para evitar danos físicos, corrupção e roubo de dados do computador, dados pessoais e software.

Responsabilidades

A gerência sênior deve assumir a responsabilidade geral pela proteção de dados e definir a prestação de contas e as responsabilidades dos funcionários da organização. Isso deve formar um documento autorizado pela gerência, indicando claramente a política, os objetivos e o compromisso de segurança total e deve levar em consideração todos os aspectos da Lei de Proteção de Dados.

As responsabilidades devem ser compatíveis com outras medidas de incêndio e segurança, a fim de garantir que não haja conflito de interesses em relação às disposições gerais de segurança.

Os procedimentos devem ser claramente definidos para a equipe que assume a responsabilidade do sistema de computador após a descoberta de corrupção de dados ou software ou violações da política de segurança da empresa que podem resultar em roubo ou mau uso da empresa ou de dados pessoais.

Controle de Usuário

Uma estação de trabalho pode compreender um terminal de computador, PC de mesa ou um dispositivo portátil, como um laptop. Todas essas estações de trabalho fornecem acesso potencial a todas as informações armazenadas na estação de trabalho e, como tal, é necessário garantir que o uso da estação de trabalho seja devidamente autorizado e controlado, usando controles físicos e de software, conforme descrito abaixo:

Acesso a estações de trabalho

- Em cada local da estação de trabalho, um indivíduo deve ser responsável por autorizar o acesso à estação de trabalho.
- Medidas devem ser tomadas para evitar a visualização ilícita de dados confidenciais ou restritos. Isso pode incluir a instalação de estações de trabalho em áreas controladas e a limpeza automática da tela após um período especificado de inatividade do teclado.
- As linhas de comunicação, soquetes, painéis de conexão e comutadores devem ser fisicamente protegidos e acessíveis somente por pessoal autorizado.
- Inventários físicos de estações de trabalho (incluindo computadores pessoais), hardware de comunicação e mídia magnética devem ser realizados em todos os locais remotos para verificar se apenas o equipamento autorizado é usado.
- Os procedimentos de segurança do laptop devem ser estabelecidos quando os laptops são retirados do escritório, ou seja, eles não devem ser deixados sem vigilância ou se deixados em um carro devem ser travados com segurança na

bota e não deixados em exibição. Idealmente, quando deixados em escritórios durante a noite, devem ser trancados em gavetas ou armários adequados.

- Deve-se considerar a proteção de equipamentos de informática de alto valor com dispositivos de segurança física, como gaiolas de segurança, barras de ancoragem ou travas de cabos de segurança.
- Visitantes, empresas de entrega e prestadores de serviços que chegam às instalações devem ser adequadamente supervisionados, com disposições de controle de acesso adequadas estabelecidas para a recepção da propriedade e para outras entradas / saídas.

Controles de acesso ao software

- Deve-se considerar o fornecimento de dispositivos de segurança física para impedir o acesso aos dados e software do computador, como dongles ou dispositivos bloqueadores de porta USB.
- A segurança do software deve incluir recursos que negam acesso a todo ou parte do sistema. Uma senha é um meio comumente usado para permitir que os sistemas de computador reconheçam um usuário autorizado. As senhas devem ser exclusivas para cada indivíduo. Senhas de grupo não devem ser usadas.
- As senhas devem ter uma complexidade proporcional à sensibilidade do acesso e devem consistir em pelo menos 6 caracteres de uma mistura alfanumérica, sempre que possível. As senhas devem ser mantidas em segredo. Em nenhuma circunstância eles devem ser exibidos centralmente ou os detalhes deixados ao lado dos terminais.
- Sugere-se que as senhas sejam alteradas da seguinte maneira:
- Em intervalos regulares, pelo menos mensalmente ou após um número especificado de logins.
- Se o usuário deixar o emprego ou for transferido para outro departamento.
- Quando a senha tiver sido revelada para outras pessoas.
- Se o comportamento do usuário exigir uma alteração.
- Tentativas de acesso com falha devem ser sinalizadas nos consoles do operador à medida que ocorrem. A equipe de segurança deve investigar falhas e negações regulares.
- A autorização de acesso para engenheiros ou pessoal de manutenção externo deve ser cancelada após a conclusão de sua tarefa.
- A gerência deve garantir que todos os usuários efetuem logoff ao sair de um terminal, mesmo por períodos relativamente curtos. Sempre que possível, os terminais devem fazer logoff automaticamente após um período predeterminado de inatividade da chave (por exemplo, 5 minutos).
- Procedimentos de aquisição de software devem ser estabelecidos para garantir que o software usado seja confiável e de uma fonte respeitável. Nenhuma aquisição não autorizada de software ou outros downloads deve ser permitida. O software adquirido deve ser verificado com os recursos adequados de verificação de vírus antes de ser introduzido nos principais sistemas de computador.
- Todos os sistemas de computador e laptops devem ser protegidos com software antivírus de boa qualidade, que deve ser atualizado regularmente.

Armazenamento de Dados e Software

As diretrizes a seguir fornecem conselhos de melhores práticas para o armazenamento seguro de dados e software:

- Os procedimentos que regulam o acesso aos dados armazenados devem minimizar a possibilidade de exibição, uso e corrupção não autorizados, modificando os nomes de arquivo padrão dos fabricantes.
- Um procedimento deve estar em operação para garantir que cópias de backup de dados e software sejam feitas e atualizadas regularmente (por exemplo, diariamente ou semanalmente), conforme necessário.
- Todas as cópias de backup devem ser verificadas quanto à validade e devem ser prontamente identificáveis.

- Idealmente, as cópias de backup devem ser mantidas fora do local ou mantidas em um gabinete de resistência ao fogo aprovado, fornecendo uma classificação mínima de duas horas. Os detalhes a seguir mostram temperaturas críticas acima das quais a mídia será danificada pelos efeitos do calor:

Discos Rígidos 65oC

- Mídia de backup off-line de curto prazo, onde é necessário um alto nível de disponibilidade, deve ser armazenada em áreas controladas por segurança.

- Os dados armazenados devem ser excluídos quando não forem mais necessários. Auditorias periódicas dos dados armazenados devem ser realizadas para garantir que nenhum dado redundante seja mantido desnecessariamente.

- Onde apropriado, os dados devem ser criptografados, em particular onde os dados estão sendo armazenados em dispositivos de memória portáteis, como CD-ROMs, cartões de memória USB ou dispositivos similares a serem retirados do escritório.

Dados impressos

Onde os dados são reproduzidos no papel ou onde os dados escritos devem ser apresentados para entrada em um computador, devem ser oferecidas as mesmas precauções de segurança que os dados armazenados. Dados impressos sensíveis, por exemplo, devem ser armazenados em armários de segurança.

Os dados impressos produzidos para desenho ou informação devem ser destruídos (fragmentados) quando não forem mais necessários. Os operadores sem a autoridade apropriada para processar informações de um determinado nível de classificação de dados não devem ter a tarefa de destruir dados impressos.

Segurança de Dados Pessoais

O aumento prolífico de uma variedade de atividades criminosas cibernéticas e outras fraudes, incluindo roubo de identidade e crimes semelhantes, fez com que as empresas prestassem uma atenção mais significativa à segurança dos dados pessoais de seus clientes, funcionários e outros terceiros mantidos em seu computador sistemas. A Lei de Proteção de Dados de 1998 cobre como as informações sobre pessoas identificáveis são usadas e seu escopo é muito mais amplo do que a Lei de 1984 anterior. Esta lei faz exigências claras às organizações em termos de segurança que deve ser aplicada para proteger os dados pessoais. A falta de proteção adequada dos dados pessoais pode resultar em processo judicial nos termos da Lei de Proteção de Dados e multas ou multas significativas. As orientações a seguir foram projetadas para minimizar os riscos da perda de dados pessoais:

- Uma política de segurança formal deve ser introduzida para identificar claramente quais informações mantidas sobre seus clientes, funcionários e outras pessoas terceiras são consideradas dados pessoais sob a Lei de Proteção de Dados. Idealmente, os dados pessoais mantidos nos sistemas do seu computador, como nomes, endereços, dados bancários e informações médicas, devem ser categorizados. As categorias podem incluir apenas altamente confidenciais, confidenciais ou internas. A política de segurança deve destacar a responsabilidade de todos os funcionários sob a Lei de Proteção de Dados para garantir a segurança dos dados pessoais mantidos em seus sistemas e essa política deve ser comunicada ativamente a todos os funcionários.

- O acesso aos dados pessoais mantidos nos sistemas de computador deve ser idealmente escalonado, com o acesso a bancos de dados (e outros aplicativos) contendo dados pessoais altamente confidenciais, como informações médicas, sendo restritos a apenas alguns funcionários com recursos de segurança de senha, conforme apropriado.

- O acesso físico ao servidor ou às salas de comunicação deve ser restrito apenas aos funcionários autorizados, com as portas sendo trancadas, por travas convencionais ou, preferencialmente, por sistemas eletrônicos de controle de acesso, que permitem o registro de todas as atividades pela porta.

- Procedimentos específicos devem ser estabelecidos para a proteção de dados pessoais retirados do escritório. Por exemplo, os laptops devem ser protegidos por senha e não devem ser deixados sem vigilância, e os dados em cartões de memória USB ou CD-ROMs devem ser criptografados.

- Os sistemas de computador devem ser adequadamente protegidos contra interferências externas e hackers. Eles devem ser protegidos por um software “firewall” adequado e proteção antivírus, incluindo o software “spy ware”.

- Se terminais ou laptops em locais fisicamente remotos, como locais de trabalho em casa, exigirem acesso à rede principal, uma conexão permanente à rede não deve ser usada. Os terminais remotos devem ser bloqueados automaticamente após um período de tempo definido. Segurança de senha adequada, para permitir a conexão às redes, também deve ser fornecida.

- Quaisquer terminais de computador obsoletos ou redundantes, laptops ou dispositivos de armazenamento de dados, como cartões de memória USB, devem ser limpos ou limpos adequadamente dos dados pessoais antes de serem descartados. Devem ser estabelecidos procedimentos para que o equipamento seja devolvido a um ponto central para permitir que os discos rígidos sejam limpos por contratados ou funcionários especializados.

- Todos os funcionários devem ser ativamente incentivados a denunciar violações da política de segurança e deve haver procedimentos formais estabelecidos para relatar e lidar com violações na segurança de dados pessoais.

Sumário

Devido à crescente dependência dos sistemas de computadores para obter mais e mais aspectos da administração de uma empresa, é provável que qualquer perda de software e dados do computador afete seriamente seus negócios. Isso pode resultar não apenas em custos financeiros adicionais para restaurar software ou dados e potencial perda de produção, mas também em danos à reputação da sua empresa e perda de confiança de seus clientes. Além disso, os calouros da Lei de Proteção de Dados podem resultar em processo judicial e pesadas multas ou sanções. Portanto, é importante proteger adequadamente todos os softwares e dados fornecidos nos sistemas do seu computador. As orientações neste Risktopic não pretendem ser exaustivas, mas são apresentadas para destacar os principais problemas e preocupações, a fim de minimizar os riscos de perda de software e dados.

Referências úteis

FPA InFiReS guidance RC3c - Recommendations for loss prevention in EDP and similar installations Part 3: Protection of Data and Software.

Contato: Risk Engineering

Zurich Brasil Seguros
Av. Jornalista Roberto Marinho, 85 - 23º andar
Brooklin Novo – 04576-010
São Paulo, SP – Brasil

Publicação do Departamento de Risk Engineering da Zurich Brasil Seguros S.A.
Edição Digital nº 01 - Atualizada em Dezembro/2020
Para receber outros informativos ou obter maiores informações, contatar o Departamento de Risk Engineering da Zurich.
E-mail: engenharia.riscos@br.zurich.com

ZURICH®