RAAS

RECOVERY AS A SERVICE

TUDO O QUE PRECISA DE SABER

PARA PROTEGER A SUA INFORMAÇÃO

CONTEÚDOS

- Introdução
- Os 7 pecados capitais de segurança nas empresas
- Segurança no mobile: as principais dicas para proteger a informação
- Como criar uma política de segurança de informação na sua empresa
- Consequências desastrosas da falta de segurança dos dados
- Perda de dados nas empresas: o que fazer para minimizar o impacto?
- Armazenamento dos dados: como reduzir os custos e aumentar a segurança?

INTRODUÇÃO

A segurança dos dados é muito importante para o sucesso dos negócios, pois cada vez mais os consumidores e demais stakeholders se preocupam com a privacidade da informação que prestam às empresas. Garantir a confidencialidade dos dados empresariais é uma luta diária dos gestores e é preciso que os colaboradores estejam alertados para a importância da segurança da informação.

Os ataques informáticos são cada vez mais sofisticados, o que faz com que os responsáveis pela segurança da informação estejam sempre alerta e que tenham uma atitude proativa no que à segurança diz respeito. Quando a segurança dos dados falha, as consequências para uma empresa podem ser desastrosas, podendo inclusivamente levá-la à falência.

Num mundo tão digital, nem sempre é fácil proteger a informação confidencial que as empresas armazenam. Devido à mobilidade, os dispositivos utilizados nas empresas são cada vez em maior número, o que faz com que seja necessário criar políticas de segurança não só para os equipamentos estáticos, mas também para os equipamentos mobile, como computadores portáteis e smartphones. E isto significa que as ameaças também existem em maior número.

Neste e-book, vamos abordar diversas questões relacionadas com a segurança dos dados nas empresas, para que possa começar a proteger, agora mesmo, o seu bem mais valioso: a sua informação!

OS 7 PECADOS CAPITAIS DA SEGURANÇA NAS EMPRESAS

1.Negligência

Apesar da crescente consciencialização da importância de proteger os dados, ainda existem muitas empresas que falham nesta área e que são negligentes no que diz respeito ao uso de um antivírus, por exemplo. Mesmo as regras mais básicas de segurança devem ser aplicadas e dadas a conhecer, pois só assim é que se consegue motivar os colaboradores a trabalhar no sentido de proteger todas as informações confidenciais.

2. Curiosidade

“A curiosidade matou o gato” é um provérbio muito antigo que deve ser levado muito a sério! Por muito tentador que seja clicar num link, não o devemos fazer se não tivermos total confiança no remetente. Muitos dos vírus instalados nos computadores entram por meio de e-mails de hackers que prometem oferecer viagens ou descontos inacreditáveis. Desconfie sempre dos e-mails que lhe prometem ofertas surreais, pois normalmente a sua origem não é fidedigna.

3. Oportunismo

Relacionado com o pecado anterior, o oportunismo é um dos maiores perigos do mundo digital. Sorteios tentadores, viagens gratuitas e obtenção de crédito muito fácil são meios que os hackers encontram para atacar os utilizadores mais inocentes. A probabilidade de se tratar de uma armadilha para roubar dados nestes casos é superior a 98%. Certifique-se de que todos os colaboradores da empresa adotam um comportamento de precaução.

OS 7 PECADOS CAPITAIS DA SEGURANÇA NAS EMPRESAS

4. Ócio

Num ambiente laboral, a Internet deve ser utilizada com objetividade e com um propósito. É certo que em algum momento todos os colaboradores usam a Internet para fins pessoais, mas há que ter muito cuidado para não se deixar levar pelo ócio. Descarregar anexos de e-mails ou entrar em sites pouco credíveis para comprar alguma coisa é bastante arriscado e pode comprometer toda a segurança da organização.

5. Inocência

Há pessoas que não desconfiam de nada ao receber inúmeros e-mails idênticos nem ao receber ofertas demasiado generosas. É preciso ter cuidado para não se ser demasiado inocente no mundo digital. Desconfie de todos os e-mails estranhos e de todos os remetentes que não conhece.

6. Indiscrição

Não confie as suas passwords a ninguém e seja bastante cuidadoso na hora de definir as suas palavras-passe. Use um gerenciador de senhas para guardar toda a sua informação privada e jamais deixe passwords expostas em post-its.

7. Desperdício

Não pode haver férias no cuidado sobre os dados privados, por isso, a segurança da informação é uma área sobre a qual deve estar sempre a trabalhar e a procurar melhores formas de garantir a sua privacidade.

OS 7 PECADOS CAPITAIS DA SEGURANÇA NAS EMPRESAS

78% das empresas em todo o Mundo sofreu pelo menos um ataque informático nos últimos dois anos

92% dos ataques sofridos acontece devido a falhas de segurança internas

35% dos ataques sofridos acontece devido a perdas de informação em dispositivos móveis

57% das empresas não protege a sua informação com soluções de proteção dos dados

61% de perda de produtividade em cada ataque informático

42% de perda de receita em cada ataque informático

RAAS
RECOVERY AS A SERVICE

SEGURANÇA NO MOBILE: AS PRINCIPAIS DICAS PARA PROTEGER A INFORMAÇÃO

Crie uma política de segurança para o mobile

Ter uma política de segurança para dispositivos móveis é fundamental para garantir o cumprimento das normas por parte dos colaboradores. Desenvolva também programas de consciencialização para a equipa, de modo a que percebam a importância de proteger os dados empresariais. Esta política de segurança deve conter sanções explícitas para os infratores, para despertar nos colaboradores o sentido de responsabilidade.

Use criptografia

Os dispositivos móveis são frequentemente conectados a redes Wi-Fi públicas e isso é bastante perigoso se não houver criptografia na hora de transferir informações importantes como nomes de utilizadores, palavras-passe, chaves para APIs, entre outras informações confidenciais.

Soluções Cloud

É difícil encontrar um negócio nos dias de hoje que tenha um horário fixo das 9h às 17h. Atualmente, as empresas são mais flexíveis relativamente a horários e devido à utilização da Cloud e da tecnologia móvel é possível trabalhar a partir de qualquer local e em qualquer momento. O armazenamento na Cloud sincroniza informações entre diferentes dispositivos, para que todos possam trabalhar na versão mais atualizada de um determinado documento, independentemente do dispositivo que estejam a utilizar e do local em que estão. A Cloud garante segurança de alto nível e máxima privacidade.

SEGURANÇA NO MOBILE: AS PRINCIPAIS DICAS PARA PROTEGER A INFORMAÇÃO

Utilize VPN

Uma VPN (rede privada virtual) é um tipo de conexão privada que utiliza uma rede pública para aceder aos dados da sua empresa. Contém uma criptografia de conexão que impede a interceção de dados e rastreamento de IP's. Esta é a forma mais segura de aceder aos dados da empresa através de redes públicas, como as dos hotéis e dos aeroportos.

Limite o acesso a recursos

Ao utilizar o seu smartphone, possivelmente vai ter que instalar diversas aplicações. Cada aplicação precisa de acesso a determinados recursos do dispositivo para funcionar corretamente. No entanto, em muitos casos as aplicações pedem acesso a recursos que não são essenciais para o seu correto funcionamento. Assim, aconselha-se que não permita que as aplicações tenham acesso a recursos que não são essenciais para a sua utilização.

COMO CRIAR UMA POLÍTICA DE SEGURANÇA DE INFORMAÇÃO NA SUA EMPRESA

A proteção da informação das empresas é o tema do momento, devido à chegada do novo regulamento geral de proteção de dados. As empresas são cada vez mais digitais e sem a prevenção da perda dos dados, a segurança destes fica seriamente comprometida. **A política de segurança nas empresas é uma ferramenta imprescindível para garantir que os seus dados permanecem seguros.**

O que é uma política de segurança?

A política de segurança é um documento desenvolvido pela empresa onde se registam os princípios de segurança que a empresa adota e que devem ser seguidos pelos colaboradores. A política de segurança deve ser aplicada em todos os sistemas de informação, a nível de desktop e de mobile. Para que a política seja respeitada, é essencial que os gestores de topo participem na sua implementação.

Como criar uma boa política de segurança da informação

- Defina a responsabilidade dos colaboradores: estabeleça coimas para a má utilização dos recursos de TI da empresa. Devem constar ainda regras sobre o acesso a sites e recomendações sobre a utilização dos dispositivos eletrónicos fornecidos.
- Dê formação: deve haver uma formação prática na apresentação da política de segurança da informação.

A empresa deve recolher declarações individuais dos colaboradores, onde se comprometem a cumprir as regras que constam no documento. Este manual deve ser de fácil acesso para os colaboradores e deverá ser revisto com frequência, para que se mantenha sempre atualizado.

COMO CRIAR UMA POLÍTICA DE SEGURANÇA DE INFORMAÇÃO NA SUA EMPRESA

- Nomeie um responsável: a empresa deve nomear uma pessoa responsável para monitorizar o cumprimento da política de segurança da informação. Este colaborador deve ser o responsável por detetar incumprimentos e violações de regras.
- Dê a conhecer a política de segurança: o documento deve ser aprovado pelo departamento de recursos humanos da empresa. As regras presentes neste documento devem estar de acordo com as leis do trabalho e com o manual interno dos colaboradores. Após a aprovação por parte dos recursos humanos, os gestores de topo também devem fazer a sua aprovação.
- Adote um plano de disaster recovery: os planos de disaster recovery são essenciais para planear ações que garantem que um desastre não interfere no desempenho da empresa. Além desta ação proativa, os planos de disaster recorvery têm também uma ação reativa, através da ação da execução de ações de emergência, planeadas previamente, e que garantem a resolução imediata de problemas. O disaster recovery define-se ainda como o conjunto de procedimentos a executar em situações de crise. O objetivo final é salvar os dados da sua empresa para que a sua informação se mantenha sã e salva.

CONSEQUÊNCIAS DESASTROSAS DA FALTA DE SEGURANÇA DOS DADOS

Os ataques informáticos são cada vez mais sofisticados, o que faz com que os responsáveis pela segurança da informação estejam sempre alerta e que tenham uma atitude proativa no que à segurança diz respeito. Quando a segurança dos dados falha, as consequências para uma empresa podem ser desastrosas.

Exposição dos dados

Quando a empresa não tem uma política de segurança dos dados eficaz, uma das piores consequências é a exposição dos dados. Se uma empresa não adotar regras de criptografia ou de mascaramento e se não proteger os seus dispositivos através de senhas, a probabilidade de dados confidenciais serem expostos é muito mais elevada. E quando este vazamento de dados acontece, a empresa perde credibilidade, podendo mesmo falir.

Multas pesadas

Com a entrada em vigor do RGPD, é preciso que as empresas tenham muito cuidado com a forma como gerem os dados mais sensíveis. O novo RGPD aposta fortemente na fiscalização e na penalização, através da aplicação de multas elevadas para os infratores. Nos casos de violações de menor gravidade poderá atingir 10 milhões de euros ou 2% do volume mundial de negócios do grupo onde a empresa se insere, e nos casos mais graves pode atingir os 20 milhões de euros ou 4% do volume de negócios mundial.

CONSEQUÊNCIAS DESASTROSAS DA FALTA DE SEGURANÇA DOS DADOS

Danos na imagem da empresa

Quando uma empresa deixa os seus dados confidenciais expostos, a sua credibilidade perante os clientes e fornecedores fica comprometida. Nenhuma empresa e nenhum cliente gosta de lidar com uma organização que não é capaz de garantir a privacidade da sua informação. Estes danos na imagem podem comprometer a sobrevivência do negócio.

Repetição do trabalho

Quando não existem garantias da proteção da informação é muito provável que as equipas de TI sejam obrigadas a fazer as mesmas tarefas várias vezes, para recuperar os dados que foram perdidos. É essencial que a empresa tenha processos bem definidos relativamente à gestão e ao tratamento dos dados confidenciais. A constante repetição de tarefas pode levar à desmotivação dos colaboradores e ao consequente aumento da taxa de rotatividade na empresa.

PERDA DE DADOS NAS EMPRESAS: O QUE FAZER PARA MINIMIZAR O IMPACTO?

No que diz respeito a perda de dados, a melhor solução é sempre a prevenção. É através dos dados que possuem que as empresas conseguem analisar o seu público, definir campanhas de marketing e orientar toda a estratégia do negócio. Contudo, existem cada vez mais ameaças à segurança da informação, pelo que é fundamental definir estratégias que permitam minimizar o impacto em caso de perda de dados nas empresas.

Backup em diferentes ambientes

É essencial que a informação mais importante da sua empresa tenha diversas cópias, para que não haja o risco de se perder para sempre. Se antigamente guardar os dados em discos externos ou em pen's era suficiente, hoje em dia aconselha-se o uso da Cloud, pois é das soluções mais fiáveis e seguras do mercado. Além de ter os seus dados guardados num local seguro, pode aceder a estes a partir de qualquer local e de qualquer dispositivo, desde que tenha acesso à Internet.

Promover o acesso condicionado

Muitas vezes as empresas não condicionam o acesso a determinados documentos por parte de alguns colaboradores e isso pode comprometer a segurança da informação. É importante que cada colaborador tenha acesso apenas aos dados de que realmente precisa, caso contrário, havendo um ataque informático, é difícil descobrir a sua origem. Também é essencial que as empresas bloqueem o acesso a informações confidenciais através de redes públicas não seguras. Deste modo, minimiza-se em grande escala a probabilidade de sofrer ataques externos.

PERDA DE DADOS NAS EMPRESAS: O QUE FAZER PARA MINIMIZAR O IMPACTO?

Ter um serviço de recuperação na Cloud

É muito importante ter um serviço de recuperação na Cloud, para que mesmo em caso de desastres informáticos não haja perda total de dados. O RAAS, por exemplo, é uma infraestrutura dedicada com replicação seletiva. Este serviço possibilita a ativação de desastre quase instantânea em servidores virtuais em ambiente remoto. Deste modo, mesmo em caso de desastres mais extremos, a informação é facilmente recuperada, não interferindo com a habitual performance da empresa.

Encriptação e mascaramento de dados

A encriptação de dados transforma a informação usando um algoritmo para que não haja um acesso fácil e percetível por terceiros, mas apenas por quem possui a chave correta de criptografia, que mostra o seu verdadeiro significado. O mascaramento de dados cria uma versão semelhante aos dados originais em termos de estrutura, mas sem revelar a sua verdadeira informação. O seu formato original mantém-se inalterado, mas os dados apresentados são fictícios. Os dados mascarados podem ser utilizados em ambientes de teste e em auditorias, não comprometendo o resultado da análise, mas garantindo sempre a confidencialidade da informação sensível. É essencial utilizar uma destas ferramentas, de modo a que mesmo que a informação seja apanhada por terceiros não consiga ser decifrada.

ARMAZENAMENTO DOS DADOS: COMO REDUZIR OS CUSTOS E AUMENTAR A SEGURANÇA?

O volume de dados criados nas empresas é cada vez maior e existe uma grande dificuldade em gerir e armazenar toda a informação criada diariamente. A tecnologia ajuda as empresas a lidar com este “boom” de dados, mas nem sempre é fácil encontrar o equilíbrio entre redução de custos e aumento da segurança.

Utilizar um bom antivírus

As empresas não devem descurar o uso do antivírus. Este deve estar sempre atualizado e é recomendado que as empresas invistam em licenças de antivírus, pois as versões gratuitas apenas oferecem um nível básico de proteção. Contudo, é importante que tenha em conta que nenhum antivírus oferece garantias de uma proteção 100% eficaz e é essencial que as empresas formem os seus colaboradores para estarem atentos a links suspeitos e para contribuírem para a proteção da informação da empresa.

Adote um storage

A utilização de um storage para consolidar os discos e centralizar o armazenamento dos dados traz imensas vantagens para as empresas. Em primeiro lugar, é um serviço escalável e consome muito menos energia do que um servidor ligado durante todo o dia, contribuindo para reduzir os custos da empresa. É um serviço seguro que utiliza a replicação dos dados, ou seja, todas as informações podem ser duplicadas em dois equipamentos distintos, eliminando a probabilidade de perda de informação. Por fim, o storage oferece um alto desempenho, visto que utiliza diferentes softwares que eliminam dados duplicados, aumentando a eficiência do sistema.

ARMAZENAMENTO DOS DADOS: COMO REDUZIR OS CUSTOS E AUMENTAR A SEGURANÇA?

Invista no armazenamento na Cloud

Um estudo levado a cabo pela KPMG concluiu que metade das empresas que opta pelo armazenamento na Cloud refere os baixos custos como o principal fator motivacional. Utilizar a Cloud vai fazer com que os documentos em meios físicos sejam eliminados, o que reduz custos com colaboradores e armazenamento. A Cloud permite que a empresa não tenha que investir em estruturas caras e complexas, como datacenters. Além disso, a utilização da Cloud é extremamente segura e permite que qualquer colaborador da empresa tenha acesso aos documentos a partir de qualquer dispositivo com acesso à Internet, o que vai melhorar a sua performance.

Defina indicadores de performance

Os indicadores de desempenho (KPI's) são muito importantes para avaliar o sucesso das estratégias utilizadas pela empresa, bem como para identificar problemas e solucioná-los. Também na área de gestão de infraestruturas e armazenamento de dados, é importante ter KPI's estabelecidos, como por exemplo, disponibilidade do sistema, qualidade dos serviços, resolução de tickets e custos de TI. O Multipeers é um excelente sistema BAM que o vai ajudar a gerir toda a informação relacionada com os indicadores, com a vantagem de poderem ser analisados em tempo real.

RAAS

RECOVERY AS A SERVICE

PHONE	+351 220 101 587
OFFICE	Rua Eng. Frederico Ulrich 3210, 1º andar. s. 101, 4470-605 Maia
EMAIL	raas.info@itpeers.com
WEBSITE	https://raas.itpeers.com/