BOM DIA PESSOAL!

acd-inc.com.br

INTRODUÇÃO AO TEMA

acd-inc.com.br

CURTO PRAZO X LONGO PRAZO

PENSE RÁPIDO

- MUITO CARO
- TODOS FAZEM O MESMO
- OUTROS SÃO MAIS BARATOS
- BILHETAGEM É SÓ UM CUSTO ADICIONAL

PENSE um pouco mais

- QUAL O VALOR AGREGADO PARA O CLIENTE?
- O QUE É IMPORTANTE PARA A OPERAÇÃO DO SEU CLIENTE?
- COMO USAR NOSSOS PRODUTOS E SERVIÇOS PARA ATENDER MELHOR SEU CLIENTE?
- COMO SUA PROPOSTA DE VALOR ESTA ALINHADA COM A NECESSIDADE DE VALOR DO SEU CLIENTE?
- VOCÊ ESTA EM COMPLIANCE COM AS LEIS?
- SERÁ QUE A MÉDIO E LONGO PRAZO O QUE PARECE BARATO NÃO FICA MAIS CARO?

ESCOLHER O CAMINHO DA NÃO CONFORMIDADE PODE SER O MAIS BARATO MAS LEMBRE-SE QUE SEMPRE HÁ A POSSIBILIDADE DE CONSEQUÊNCIAS SÉRIAS.

TIME ACDI

PaperCut Certified Authorized Solution Center

Discurso de Parceiro para
Segurança de Impressão

https://www.uol.com.br › 2021/06/08 ▾ Translate this page

Vazamento expõe 8,4 bilhões de senhas e pode ser o maior ...

Jun 8, 2021 — Antes do **RockYou2021**, o título de maior **vazamento de dados** da história era do COMB (Compilation of Many Breaches), que expôs 3,2 ...

https://tiinside.com.br › 2021 › inves... ▾ Translate this page

Investimento em segurança cibernética pode acelerar a ...

Jun 4, 2021 — **Investimento** em **segurança** cibernética pode acelerar a transformação ... **Investir em Cyber** é essencial para alavancagem dos negócios", destaca André ... As respostas foram coletadas entre fevereiro e março de **2021**.

https://g1.globo.com › tecnologia › noticia › 2021/01/28

Megavazamento de dados de 223 milhões de brasileiros: o ...

... com CNPJs. Origem dos **dados** ainda é desconhecida. ... Por G1. 28/01/**2021** 18h34 Atualizado há 2 meses ... Como proteger meus **dados** de **vazamentos**?

NASA

> Um dos ambientes mais seguros e visados por criminosos digitais conta com o PaperCut MF e o time ACDI para manter a tranquilidade dos seus dados seguros.

- **Ransonware**

É um dos ataques mais utilizados ultimamente no mundo todo, é um processo que infecta o sistema da vítima e bloqueia o uso de todos os dados e exige um **resgate**, normalmente em criptomoedas. De acordo com um relatório da **CISCO** de 2017 é o **tipo de ataque mais rentável da história**. O primeiro relato documental desde tipo de ataque foi em 2005 do Estados Unidos.

- Phishing & Spoofing

Ataques voltados para engenharia social e que se utiliza da confiança de uma marca ou indivíduo para roubo dos dados. Utilizando técnicas de design você acha que esta mesmo falando com uma empresa ou pessoa mas na verdade é outra.

- URL

Utiliza-se de técnicas antigas e sistemas com problemas de desenvolvimento que apenas “escondem" endereços dos usuários, sem um desenvolvimento estruturado pode comprometer acesso a dados confidenciais de uma maneira super simples.

- Decoy

Aqui o ataque é mais bem pensado quanto ao acesso a um sistema “idêntico" ao que o usuário esta acostumado a usar mas na verdade é um sistema preparado para roubar seus dados. Muito comum em Internet Banking.

Discurso de Parceiro para

Segurança de Impressão

O MPS não esta imune a ataques, muito pelo contrário

Discurso de Parceiro para

Segurança de Impressão

"O MPS trafega algo em torno de 1000x a mais dados sensíveis e confidenciais do que outras soluções"

Discurso de Parceiro para

Segurança de Impressão

OS 5 MANDAMENTOS

5 MANDAMENTOS

- CONFIDENCIALIDADE

Informação só pode ser acessada e atualizada por pessoas autorizadas e credenciadas.

- CONFIABILIDADE

É o caráter de fidedignidade da informação. Deve ser assegurada ao cliente a boa qualidade da informação com a qual ele esta trabalhando.

- INTEGRIDADE

É a garantia de que a informação estará completa, exatas preservada contra alterações, manipulações manuais, fraudes ou até contra destruição.

- DISPONIBILIDADE

É a garantia de que a informação estará acessível e disponível em escala contínua para as pessoas autorizadas e de direito.

- AUTENTICIDADE

É o saber, por meio de registro apropriado, quem realizou acessos, atualizações, exclusões de modo que haja confirmação da autoridade e originalidade

PONTOS IMPORTANTES

- ## CLOUD

Soluções de Impressão em Cloud precisam seguir mais políticas do que outras pois além de trafegarem dados sensíveis em uma quantidade maior (job a job) carregam dados confidenciais e ainda pacotes de autenticação 1000x mais do que outras soluções cloud.

- ## BANCO DE DADOS

A localização do banco de dados é fundamental pois, em soluções em impressão, o banco de dados possui os dados de bilhetagem que são o objetivo-fim de uma solução de billing. Se ele esta em cloud, a fornecedora tem co-responsabilidade em qualquer atividade e tempo de resposta LGPD.

- ## PROPRIEDADE

A propriedade dos dados é sempre do cliente final e ele precisa ter, de forma transparente, como as atividades em cima desses dados são aplicadas, se os dados ficarem em cloud o risco aumenta muito pois toda a cadeia de fornecimento é responsável por manter os 5 mandamentos e políticas.

- ## RESPONSABILIDADE

A responsabilidade dos dados é de quem os armazena, portanto, em vazamentos, ataques a cadeia de fornecimento é obrigada a avisar pró-ativamente o cliente, garantir novas políticas de proteção e ainda arcar com todas as possíveis sanções legais que podem ser aplicadas.

- ## POLÍTICAS

É um conjunto de práticas, definidas com o DPO (falaremos do DPO mais a diante) de como além de cuidar dos dados, quais funcionalidades precisam ser aplicadas como anonimizar dados, não visualizar determinadas informações e ainda é ele quem precisa ser avisado sobre qualquer falha ou ataque já que ele responde legalmente pela LGPD dentro da empresa.

FIM SLGPD-01

acd-inc.com.br