O QUE É PRECISO **PROTEGER** DENTRO DA SUA EMPRESA?

ATHENA
SOLUÇÕES INTELIGENTES

SÚMARIO

ATHENA
SOLUÇÕES INTELIGENTES

Introdução

É impossível ignorar a enxurrada de notícias sobre violações de segurança cada vez mais frequentes e, na maioria das vezes, bem-sucedidas, ao longo dos últimos meses. Um fato é inquestionável: o mundo mudou e a forma de se trabalhar também. Como consequência? Os incidentes de segurança também acompanharam os novos tempos.

Em meio à uma pandemia que não dava sinais de trégua, 2021 começou com um megavazamento de 223 milhões de dados de brasileiros, número maior do que a população do país (estimada em 212 milhões), já que também incluía dados de pessoas falecidas. Desde então, quase semanalmente vem à público alguma notícia de ataques a empresas de todos os tipos de segmento e porte. Tais incidentes confirmam que os ataques aumentaram, mas as detecções também.

AS **AMEAÇAS CIBERNÉTICAS** DEIXARAM DE SER APENAS AMEAÇAS

De acordo com o Breach Level Index, mais de 9,7 bilhões de registros de dados foram perdidos ou roubados, em todo o mundo, desde 2013 como resultado de violações de dados e crimes cibernéticos.

7 MILHÕES
de dados comprometidos **todos os dias**

56 REGISTROS
comprometidos a **cada segundo**

$3.26 MILHÕES
é o **custo médio** global de uma violação de dados

ATHENA
SOLUÇÕES INTELIGENTES

PAINEL DE **ATAQUES CIBERNÉTICOS NO BRASIL**

JANEIRO

UBIQUITI NETWORKS

Ubitiqui sofre violação de sistemas de segurança

Link

FEVEREIRO

COPEL

Em comunicado, Copel confirma ataque cibernético

Link

MARÇO

Shell comunica incidente de segurança

Link

ABRIL

iugu

Novo vazamento de dados expõe clientes da empresa iugu

Link

ATHENA SOLUÇÕES INTELIGENTES

MAIO

- Ransomware segue gerando caos na indústria e JBS se pronuncia sobre ciberataque

  Link

- JBS retoma operação após ataque ransomware

  Link

- JBS paga US$ 11 milhões de resgate após ataque ransomware

  Link

JUNHO

- Grupo Fleury sofre ataque externo

  Link

- Fleury não confirma pagamento de resgate e segue restabelecendo sistemas

  Link

JULHO

- Grupo Protege sofre tentativa de ataque cibernético

  Link

ATHENA SOLUÇÕES INTELIGENTES

AGOSTO

Accenture é vítima de ataque cibernético

Link

SETEMBRO

Site da Anvisa volta à normalidade após ataque cibernético

Link

OUTUBRO

Porto Seguro sofre tentativa de ataque cibernético

Link

NOVEMBRO

Panasonic comunica invasão criminosa de servidor

Link

DEZEMBRO

Correios sofre ciberataque e LAPSUS$ assume autoria

Link

VIRANDO O JOGO

Segundo a pesquisa Global Digital Trust Insights 2021, da PWC, “os líderes de segurança estão trabalhando em estreita colaboração com as equipes de negócio para fortalecer a resiliência da organização como um todo. Como resultado, as áreas de segurança da informação estão equilibrando forças com os invasores, resistindo e se defendendo como nunca antes”.

Tal cenário mostra que as empresas sabem que precisam investir em segurança da informação e sabem também que não têm tempo a perder. Mas, por onde começar? A resposta é simples: **sabendo o que é preciso proteger.**

ATHENA
SOLUÇÕES INTELIGENTES

PARA COMEÇAR: DLP – DATA LOSS PROTECTION

A segurança dos dados é um desafio constante para as empresas:

1° Proteger os dados contra ataques direcionados.

2° Atender aos órgãos regulamentadores (LGPD, BACEN, SUSEP, dentre outros), para os quais é necessário ter visibilidade do que acontece com as informações confidenciais.

3° Adaptar-se às mudanças no formato de trabalho (remoto, híbrido), assim como a adoção de aplicativos em nuvem, ambientes de nuvem híbridos e a prática do BYOD (*Bring your own device*), que aumentam as formas como os dados podem sair da organização.

Para tanto, a abordagem vai além de identificar os dados, catalogá-los e controlá-los. A adoção de um software de DLP deve ir além dessa fase, considerando a maior das variáveis em segurança: as pessoas. Ou seja, o programa de proteção de dados de uma organização deve considerar o ponto humano - a interseção de usuários, dados e redes. Além disso, a empresa deve manter a vigilância sobre os dados que percorrem a empresa e destacar as pessoas que criam, tocam e movimentam dados.

ATHENA SOLUÇÕES INTELIGENTES

Com isso, a adoção de um software de DLP deve considerar primordialmente:

- Proteger dados regulados com um ponto de controle único para todos os aplicativos que os colaboradores usam para criar, armazenar e movimentar dados.
- Proteger a propriedade intelectual analisando como os colaboradores usam os dados.

Na prática, no entanto, o processo pode ser desafiador para as empresas, uma vez que enfrentam desafios como:

- Equipes internas com baixo conhecimento em classificação de dados
- Equipes enxutas com diversas responsabilidades
- Baixa compreensão de que DLP é apenas para setores críticos, como os departamentos financeiro ou de pesquisas

Por isso, ter um parceiro que consiga trazer a cultura para a empresa, rompendo barreiras, pode fazer toda diferença para o sucesso do projeto.

ATHENA
SOLUÇÕES INTELIGENTES

E SE A **FÓRMULA DA COCA-COLA** VAZASSE?

Mas antes de estruturar um projeto de DLP, é preciso que fique muito claro seu propósito. A adoção de um software de DLP é para atender a LGPD? Não! Pelo menos, não apenas. A LGPD (Lei Geral de Proteção de Dados) estabelece diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. E aqui vale ressaltar: dados pessoais.

Mas, você já pensou se a fórmula da Coca-Cola vazasse? Ela não é um dado pessoal, mas trata-se (talvez) da informação mais importante da empresa. E os segredos de Estado de um governo? Não são cadastros de contato, mas seu uso inadequado pode trazer sérios riscos à instituição.

Com esses exemplos é possível entender **o quão importante é proteger determinadas informações** e que suas violações transcendem os riscos de eventuais multas previstas pela LGPD. Elas podem levar a empresa à sérios danos financeiros e de imagem.

DLP DA Forcepoint

O Forcepoint DLP aborda o risco centrado nas pessoas com visibilidade e controle em todos os lugares onde elas trabalham e em todos os lugares onde os seus dados residem. As equipes de segurança aplicam pontuação de riscos de usuários para ter foco nos eventos mais importantes e acelerar a conformidade com as regulamentações de dados globais.

Acelerar a conformidade

O ambiente de TI moderno apresenta um desafio intimidador para as empresas que procuram cumprir dúzias de regulamentações de segurança de dados mundiais, especialmente à medida que migram para aplicativos de nuvem e adotam forças de trabalho móveis. Muitas soluções de segurança oferecem alguma forma de DLP integrado, como o tipo encontrado em aplicativos de nuvem.

Contudo, as equipes de segurança enfrentam complexidade indesejada e custos adicionais ao implementar e administrar políticas separadas e inconsistentes entre endpoints, aplicativos de nuvem e redes. O Forcepoint DLP acelera os seus esforços de comformidade, combinando cobertura em pacotes predefinidos para as regulamentações globais com controle central em todo o seu ambiente de TI. Além disso, protege com eficiência as informações confidenciais de clientes e os dados regulados, para que o cliente possa comprovar com confiança a conformidade constante.

Habilitar as pessoas para proteger os dados

O DLP que só contém controles preventivos frustra os usuários, que vão contorná-los com a intenção exclusiva de concluir uma tarefa. Contornar a segurança resulta em um risco desnecessário e exposição de dados involuntária. O Forcepoint DLP reconhece as pessoas como as vanguardas das ameaças digitais atuais.

Detecção avançada e controles que seguem os dados

As violações de dados maliciosas e acidentais são incidentes complexos, não são eventos únicos. O Forcepoint DLP é uma solução comprovada que empresas de análises (incluindo Gartner, Radicati e outras) reconhecem como líder no setor.

Identificar, administrar e corrigir o risco de proteção de dados

As abordagens tradicionais para DLP sobrecarregam os usuários com falsos positivos e deixam de identificar dados em risco. Além de reduzir a eficácia das equipes de segurança, isso frustra os funcionários ou os usuários finais, porque eles consideram as soluções de segurança como um obstáculo à sua produtividade nos negócios.

Com as análises, o Forcepoint DLP reduz os falsos positivos, o que ajuda nas operações de segurança. Para aumentar a conscientização de segurança dos funcionários, o DLP disponibiliza orientação de funcionários e integração com soluções de classificação de dados.

Visibilidade em todos os lugares onde as pessoas trabalham, controle em todos os lugares onde os seus dados residem

Atualmente, as empresas enfrentam os desafios de ambientes complicados, em que os dados estão em todos os lugares, e precisam de proteção de dados em lugares que não são administrados ou de propriedade da empresa. O Forcepoint DLP for Cloud Applications amplia as análises e as políticas de DLP para aplicativos de nuvem críticos, de forma que seus dados sejam protegidos, não importa onde residam.

ATHENA
SOLUÇÕES INTELIGENTES

ATHENA
SOLUÇÕES INTELIGENTES

SOBRE A ATHENA SOLUÇÕES INTELIGENTES

Somos uma consultoria com foco em GRC | IRM – Governança, Riscos e Compliance, Segurança da Informação e LGPD, formada por profissionais certificados e altamente experientes na condução de serviços e implementação de soluções próprias e de parceiros.

Utilizamos soluções robustas, líderes no quadrante mágico do Gartner e com ampla presença na nossa região.

Em nosso portfólio – Athena Professional Services – atuamos fortemente com Implementação de Soluções, Serviços Pós Implementação de Soluções, Auditorias e Gap Analysis, Treinamentos e Consultoria, com clientes de todos os segmentos de mercado em todo o país.

Nosso desafio é construir soluções inteligentes e inovadoras para ofertar ao mercado o que há de mais moderno e atualizado em GRC | IRM, Segurança da Informação e LGPD.

https://www.athenasolucoes.com

ATHENA
SOLUÇÕES INTELIGENTES

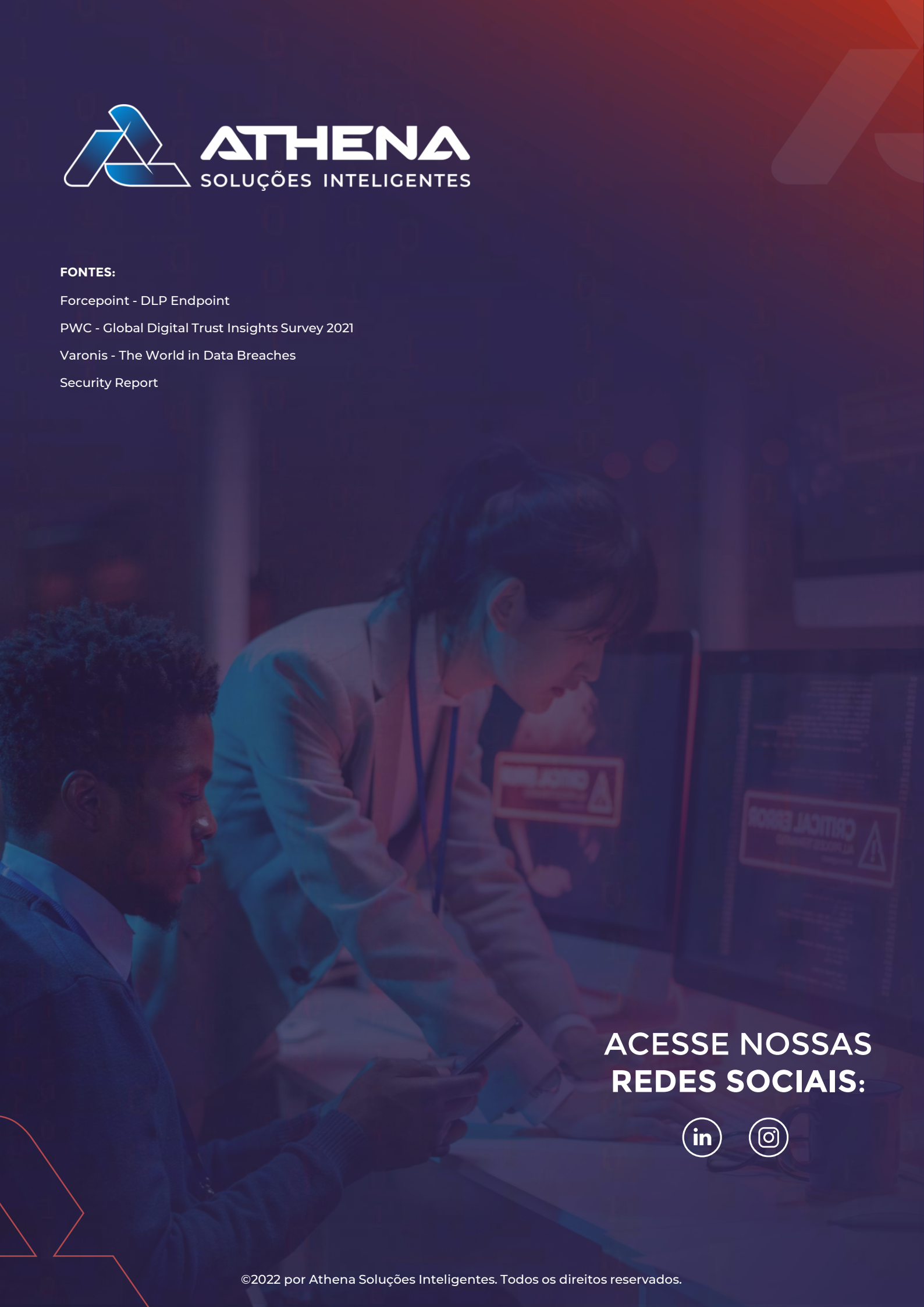
FONTES:

Forcepoint - DLP Endpoint

PWC - Global Digital Trust Insights Survey 2021

Varonis - The World in Data Breaches

Security Report



ACESSE NOSSAS REDES SOCIAIS: