Marsh

Incidentes Cibernéticos

Resposta a incidentes envolvendo dados pessoais e como mitiga-los.

Maio de 2024
Fabiano Totino – Cyber Claims Specialist

- Incidentes ocorridos nos últimos anos – Nossos indicadores;
- Indicadores globais - Custos com violação de dados;
- Como responder e mitigar essas ameaças?;
- *Cases* de incidentes envolvendo dados pessoais;

Programação

Incidentes Cibernéticos ocorridos nos últimos anos

+BRL 500MM

Em prejuízos reclamados decorrentes de incidentes cibernéticos envolvendo dados pessoais.

+70

Incidentes atendidos ao longo dos últimos 3 anos.

+ 20MM

Dados de clientes expostos e disponíveis gratuitamente em fóruns na *Deep & Darkweb* em um único incidente

80%

Dos incidentes reportados estão relacionados a ataques de *Ransomware*.

11

Número de países simultáneamente afetados em incidente com exfiltração de dados pessoais.

80%

Dos incidentes já indenizados tiveram paralização total ou parcial das atividades.

Indicadores Globais – Cost of a Data Breach Report 2023 - IBM

US$ 4,45MM

Custo médio global de uma violação de dados em 2023, um aumento de 15% ao longo de 3 anos.

553

Organizações atingidas por violações de dados entre março de 2022 a março de 2023.

US$ 3,84MM

Custo médio de violação de dados das organizações que relataram baixa ou nenhuma complexidade do sistema de segurança.

51%

Das organizações planejam aumentar os investimentos em segurança por conta de uma violação que sofreram, incluindo planejamento e teste de resposta a incidentes (RI), treinamento de funcionários e ferramentas de detecção e resposta a ameaças.

57%

Das empresas disseram que eram mais propensas a repassar os custos associados aos ataques aos consumidores, em vez de aumentar seus investimentos em segurança.

95%

Das organizações pesquisadas sofreram mais de uma violação.

Marsh

Como responder esses incidentes?

Como mitigar esses incidentes com dados pessoais?

Faça backup continuamente e mantenha seus sistemas de TI sempre atualizados;

Armazene dados pessoais com segurança. Senhas fortes, restrição de acesso e o monitoramento de ambientes são maneiras de aumentar a segurança no meio digital e no meio físico;

Uma outra boa prática na gestão de incidentes para os agentes de tratamento, encontrada em *frameworks* de segurança da informação é a realização de exercícios de simulação de incidentes (*Tabletop*).

Os riscos à segurança física dos ambientes corporativos, ambientes críticos, como o centro de dados (*data center*) e salas de arquivo de guarda de documentações em papel, como prontuários médicos de funcionários e prestadores de serviço.

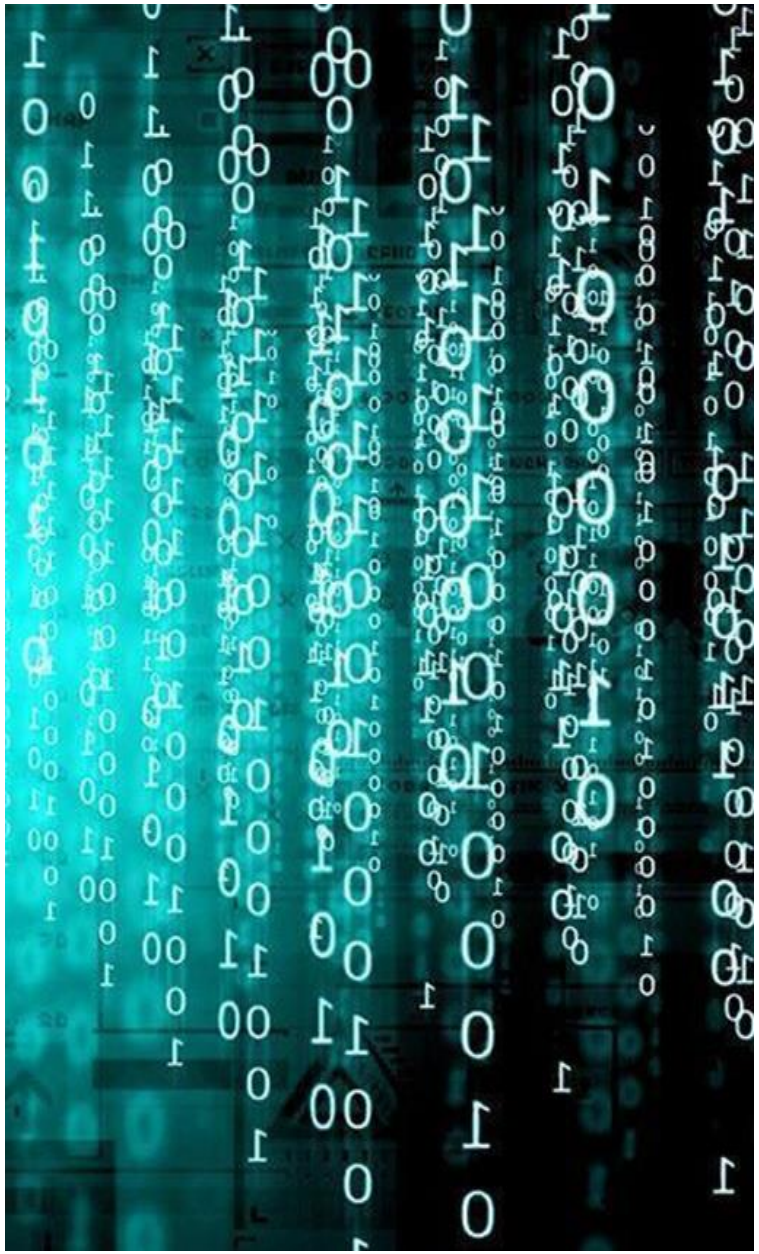
Como mitigar esses incidentes com dados pessoais?

Mapeamento dos processos internos da empresa e identifique os pontos críticos que geram mais riscos. Desenvolva uma política interna com as regras e procedimentos de segurança de informação;

Controle de acesso aos sistemas de TI, criando diferentes perfis de colaboradores dentro da própria empresa e garantindo que os funcionários tenham acesso apenas aos dados e sistemas necessários para o desempenho de suas funções;

Regras para o trabalho remoto. Há um relaxamento natural dos colaboradores quando trabalham fora da empresa. Procure sempre lembrá-los da importância da manutenção das políticas de segurança dentro e fora das dependências da empresa.

Revisão periódica dos dados de seus clientes, mantendo-os sempre atualizados ou descartando os que não são mais necessários. Realize treinamentos contínuos, é fundamental que os colaboradores saibam e coloquem em prática os procedimentos de segurança e as boas práticas da empresa;



Cases de incidentes envolvendo dados pessoais

https://oglobo.globo.com/economia/tecnologia/noticia/2024/01/26/central-dos-vazamentos-na-internet-reu...

LOBO | Tecnologia ASSIN

'Central dos vazamentos' na internet dados de 26 bilh

https://www.cisoadvisor.com.br/vazamento-do-

Canais Branded Posts Podcasts

Vazamento do [redacted] 20 milhões de dad

Os dados de registros de clientes da agência de viagens online [redacted] na dark we

Erivelto Tadeu
28/07/2020

Mais de 20 milhões de registros de clientes da agênci[redacted]) estão disponíveis gra

A violação foi descoberta pela equipe da unidade [redacted] fornecedora global de ferramentas voltadas à inteli[redacted] Atlanta, EUA.

Marsh

https://www.cisoadvisor.com.br/[redacted]-e-anunciada-como-vitima-do-grupo-lapsus/

[redacted]é anunciada pelo grupo Lapsus$ como vítima

Grupo redirecionou visitantes do endereço da empresa para um site de pornografia

[redacted]aulo Brito
[redacted]/01/2022

[redacted]tícia atualizada às 15h30

[redacted]grupo Lapsus$, que atacou o Ministério da Saúde, a Claro, os Correios, anunciou nesta madrugada [redacted] atacado as operações de internet da [redacted] considerada a maior empresa de aluguel de veículos [redacted] América Latina. O anúncio foi feito às 02:43 de hoje pelo canal do Telegram mantido pelo grupo. [redacted]arentemente o ataque foi feito aoenas contra os serviços expostos na web: na mensagem que [redacted]uncia o incidente, o grupo acrescentou uma descrição do site de pornografia PornHub – numa [redacted]licação de que os visitantes do endereço original da Localiza estariam sendo redirecionados para [redacted]se outro endereço.

https://boaforma.abril.com.br/fitness/dados-de-150-milhoes-de-usuarios-de-app-fitness-vazam-na-web

Dados de 150 milhões de usuários de app fitness vazam na web

Saiba o que fazer se você usa o [redacted]um dos aplicativos mais populares na categoria saúde e fitness

POR CAMILA JUNQUEIRA, GISLENE PEREIRA
ATUALIZADO EM 3 MAIO 2024, 10H11 - PUBLICADO EM 2 ABR 2018, 19H56

Soluções Serviços Parc

[redacted]ustou R$230 milhões à[redacted]Brasil.

[redacted]maiores provedores em nível mundial de serviços de gestão de [redacted]e terceirização de processos de negócios (CRM/BPO) e líder na América [redacted]021, sofreu um ataque hacker que causou um enorme impacto financeiro a [redacted]

[redacted]a operação brasileira, com impacto contabilizado em US$ 46,1 milhões – [redacted]

[redacted]s para reverter a ação criminosa e de perda de receita por conta do [redacted]partir do incidente cibernético. O impacto foi tão forte que a operação [redacted]na sua receita, mas acabou sem crescimento em relação ao ano passado.

[redacted]s clientes tiveram que acionar "o plano B", ou assumirem a gestão de [redacted]i, no entanto, não revelou qual o incidente cibernético sofrido, não [redacted]somware ou malware.

[redacted]e Lockbit 2.0 publicaram no dia 31/10/2021 em seu site de vazamentos [redacted]iretórios contendo arquivos supostamente roubados da empresa [redacted] O [redacted]a que todos os dados obtidos foram publicados.

Dúvidas