

>>> Principais Ataques à Segurança da Informação na Atualidade
>>> Redes II

Name: j.martins[†]-pigor[‡] (@pucminas)
Date: 10 de março, 2024

[†]João Victor Martins Medeiros

[‡]Pedro Igor Martins dos Reis

```
>>> Western Digital
```

[illegible]

>>> Western Digital¹

- * Fundada em 1970;
- * Atuação em nível global;
- * 20B USD em valor de mercado;
- * Fabricante de diversas soluções de armazenamento;
- * Grupo formado por mais 4 subsidiárias:
 - * WD;
 - * WD_Black;
 - * SanDisk;
 - * SanDisk Professional.

¹<https://www.westerndigital.com/>

```
>>> Alpv, a.k.a BlackCat
```

[illegible]

- * 26 de março de 2023;
- * 10TB de dados internos e SAP *Backoffice* roubados [Abr23];
- * Serviços em nuvem^a temporariamente desligados;
- * *"We know you have the link to our onion site. Approach with payment prepared, or **** off. Brace yourselves for the gradual fallout."* [Alv23];
- * *"We will **** you until you cannot stand anymore Western Digital. Consider this our final warning."* [Fra23];

^aMy Cloud, My Cloud Home, My Cloud OS 5, ...

>>> Medidas preventivas

- * Treinamento de funcionários;
- * Auditorias internas regulares;
- * Estratégias de resposta a incidentes;
- * Fortalecimento de sua infraestrutura interna.

Considere o ataque cibernético sofrido pela Western Digital em 2023, qual das seguintes afirmações é incorreta?

- * A) A Western Digital utilizou o incidente como uma oportunidade para melhorar suas práticas de segurança cibernética, implementando criptografia de arquivos em toda a sua rede como medida de proteção contra futuros ataques.
- * B) O grupo de *ransomware* 'Alphv', também conhecido como 'BlackCat', assumiu a responsabilidade pelo ataque, utilizando o incidente para extorquir a empresa, ameaçando publicar os dados roubados.
- * C) O ataque resultou na exfiltração de aproximadamente 10 terabytes de dados da empresa, incluindo informações detalhadas de clientes, e os hackers exigiram um resgate de oito dígitos.
- * D) A Western Digital desativou temporariamente alguns de seus serviços para conter a ameaça e iniciou uma investigação com especialistas em cibersegurança e autoridades policiais.

Considere o ataque cibernético sofrido pela Western Digital em 2023, qual das seguintes afirmações é incorreta?

- * A) A Western Digital utilizou o incidente como uma oportunidade para melhorar suas práticas de segurança cibernética, implementando criptografia de arquivos em toda a sua rede como medida de proteção contra futuros ataques.
- * B) O grupo de *ransomware* 'Alphv', também conhecido como 'BlackCat', assumiu a responsabilidade pelo ataque, utilizando o incidente para extorquir a empresa, ameaçando publicar os dados roubados.
- * C) O ataque resultou na exfiltração de aproximadamente 10 terabytes de dados da empresa, incluindo informações detalhadas de clientes, e os hackers exigiram um resgate de oito dígitos.
- * D) A Western Digital desativou temporariamente alguns de seus serviços para conter a ameaça e iniciou uma investigação com especialistas em cibersegurança e autoridades policiais.

>>> Referências

- [Abr23] Lawrence Abrams. *Hackers leak images to taunt Western Digital's cyberattack response*. <https://www.bleepingcomputer.com/news/security/hackers-leak-images-to-taunt-western-digitals-cyberattack-response/>. Acessado em: 10-03-2024. 2023.
- [Alv23] Dominic Alvieri. *Avisos para Western Digital*. <https://twitter.com/AlvieriD/status/1648133899766099974>. Acessado em: 10-03-2024. 2023.
- [Fra23] Lorenzo Franceschi-Bicchierai. *Hackers claim vast access to Western Digital systems*. <https://techcrunch.com/2023/04/13/hackers-claim-vast-access-to-western-digital-systems/>. Acessado em: 10-03-2024. 2023.