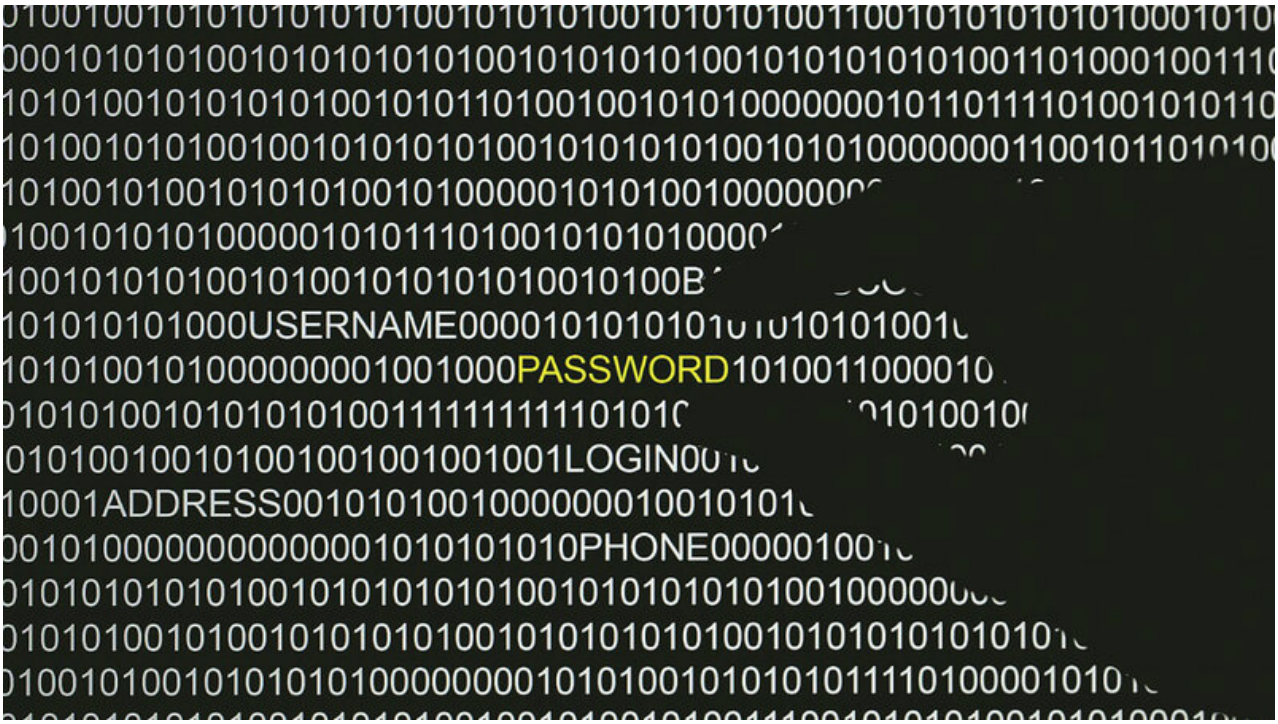
Lições retiradas do ciberataque à Câmara Municipal de Vinhais

dinheirovivo.pt/opiniao/licoes-retiradas-do-ciberataque-a-camara-municipal-de-vinhais-12775717.html

5 de novembro de 2019



A Câmara Municipal de Vinhais, no distrito de Bragança, sofreu no mês passado um ataque informático que comprometeu os seus serviços durante mais de uma semana. O autor do ataque terá encriptado os dados da autarquia, exigindo um resgate bastante elevado pela sua desencriptação.

Pelo que fui acompanhando na imprensa, em causa esteve um tipo de ciberataque, o ransomware, cada vez mais popular por todo o mundo e, em particular, junto de câmaras municipais, escolas ou hospitais. Aliás, pela mesma altura deste ataque, foi noticiado que, só este ano, mais de 30 organismos públicos terão passado por algo semelhante.

Este tipo de ataque é particularmente inconveniente porque, por norma, para além de conseguir "roubar" informação, tem ainda a capacidade de condicionar ou até paralisar os serviços que dependam dessa mesma informação, o que resulta em constrangimentos graves para colaboradores, clientes e fornecedores da organização atacada. No caso da câmara de Vinhais, por exemplo, coincidiu com o processamento de salários dos funcionários municipais.

Enquanto acompanhava os relatos do sucedido, não pude deixar de refletir sobre algumas lições que podemos obter deste ataque. Vejamos:

Em primeiro lugar, o presidente da autarquia não pagou o resgate. Efetivamente, esta é uma prática recomendada em caso de ataques *ransomware*, pois, em primeira instância, nada garante que o pagamento do resgate leve ao efetivo desbloqueio da informação e,

mais importante, a opção de não colaborar com o crime ao pagar o resgate acaba por "esgotar" o modelo de negócio dos atacantes e, portanto, acaba por ser uma ação recomendada na perspetiva de não promover o crime. Adicionalmente, o valor do resgate será, em princípio, bastante superior à contratação de ajuda legítima externa.

Depois, a autarquia informou as autoridades competentes e contratou especialistas em cibersegurança para a auxiliarem no processo de investigação e posterior recuperação da informação e do serviço afetado. Esta é outra prática recomendada, pois estamos perante um crime e este género de crimes têm enorme impacto e complexidade, o que exige *know how* e domínio de ferramentas especializadas que não estarão, em princípio, ao alcance da organização atacada.

Por fim, não "abafou" o incidente, tendo falado abertamente sobre o mesmo. Ainda que não se trate de uma prática recomendada e nem sempre seja necessário ou até recomendável tornar público um incidente deste tipo, é um gesto fundamental para alerta e sensibilizar os pares.

A ausência de cultura de cibersegurança ou o investimento deficitário em cibersegurança leva, muitas vezes, a situações como a que ocorreu na Câmara Municipal de Vinhais. Além da qualidade dos serviços e do acesso ilegítimo a informação sensível ou pessoal (atenção ao cumprimento e conformidade legal obrigatória face ao RGPD!), é a própria credibilidade das instituições que é posta em causa.

De facto, é realmente responsabilidade das organizações garantir que o risco de ataque informático é o mínimo possível, tal como é implementado pela segurança física das suas instalações ou dos seus colaboradores, clientes ou fornecedores. Mas, para que isso seja possível, é essencial que a consciência do risco exista pela estrutura de gestores e decisores das organizações, e depois, se disponham a avaliar continuamente a capacidade preventiva e reativa de cibersegurança das suas infraestruturas tecnológicas, aplicacionais e humanas.

Ao denunciar o ataque, o presidente da câmara de Vinhais contribuiu para que outras organizações estejam mais alerta para a necessidade de cibersegurança, principalmente quando a transformação digital é cada vez mais parte integrante da vida das pessoas e das organizações. E contribuiu, ainda, para a sociedade civil ouvir falar de conceitos como ataques de phishing, ransomware ou, mesmo, de cibersegurança.

Sofrer um ciberataque não deve ser "um embaraço", sobretudo quando não se está ainda preparado para tal. Contudo, deve ser uma oportunidade para aprender, corrigir e não repetir, no futuro, os erros do passado.

Bruno Castro é CEO da VisionWare