"Não é aceitável". Página de acesso aos certificados de aforro é vulnerável a ciberataques?

poligrafo.sapo.pt/fact-check/nao-e-aceitavel-pagina-de-acesso-aos-certificados-de-aforro-e-vulneravel-a-ciberataques

Salomé Leal 22 de maio de 2023

https://twitter.com/tomahock/status/1637819952190062598

"Já que os certificados de aforro estão na moda, vamos olhar para a página de login do AforroNet. O *user* é uma *string*. O código de acesso é um número com seis algarismos. E pedem dois números do NIF. Esta página está **completamente vulnerável a ataques de *brute force***", alerta-se num "tweet" de 20 de março. A denúncia já correu o Reddit, o Facebook e também chegou ao Polígrafo. Afinal, quão fácil seria fazer uma autenticação de terceiros neste portal da Agência de Gestão da Tesouraria e da Dívida Pública (IGCP)?

Pouco, garante ao Polígrafo fonte oficial do IGCP: "O Aforronet beneficia de vários mecanismos de segurança. A arquitetura de acesso ao AforroNet **bloqueia as contas em caso de tentativas de acesso múltiplas**. A atividade de acesso às contas aforro é rastreada e monitorizada, sendo espoletados protocolos de ação quando a atividade de acesso é considerada anormal. São ainda promovidos testes e atualizações regulares ao sistema de informação."

Em suma, por mais simples que seja acertar numa combinação de seis dígitos, a verdade é que o portal só oferece **três tentativas**. Ao fim das mesmas, o acesso à conta fica bloqueado e só sai deste estado depois de ser enviada uma **carta com novo código** ao proprietário da conta. Suficiente? Bruno Castro, CEO da VisionWare, empresa portuguesa especializada em segurança de informação, diz que não.

"Até eu fiquei surpreendido com este nível de maturidade. Não é aceitável. Aquele tipo de autenticação que está montado é completamente rudimentar e **não era suposto vermos isso nos dias de hoje em *sites* do Estado**. Isto é um facto. Esta nem tem sido a tendência do próprio Estado", garante o especialista ao Polígrafo. Os perigos são claros: "a imagem do Estado e da instituição em causa e tudo o que está lá dentro, que pertence a pessoas que o Estado tem obrigação de proteger."

Sobre soluções, Bruno Castro explica que a autenticação na área da segurança compreende essencialmente três mecanismos: "O que nós sabemos, *password*, por exemplo; o que nós temos, pode ser um telefone; e o que nós somos, retina ou impressão digital. Qualquer um destes mecanismos, isolado, resulta numa autenticação fraca. Dois destes juntos, passa para autenticação forte. Neste tipo de acessos, tendo em consideração a imagem da instituição e o conteúdo que está lá dentro, **pedia-se no mínimo uma autenticação forte**. Uma password com 8,9, 12 caracteres, inclusive especiais, uma coisa minimamente atual. E por cima disto ou o que 'nós temos' ou o que 'nós somos'."

Mais do que um perigo a nível pessoal, há a imagem de uma instituição que a quer preservar: "Se eu estou interessado no conteúdo que está lá dentro, ou quero pôr em causa a imagem da instituição, **basta que bombardeie completamente com tentativas falhadas** e, de repente, tenho 100mil utilizadores bloqueados. Tem o mesmo impacto, em termos mediático, que o site não estar a funcionar."

Questionada pelo Polígrafo sobre este tema, a Dark Clarity, empresa especializada em cibersegurança, realizou uma **avaliação não intrusiva ao sistema de autenticação do site AforroNet**. As conclusões foram as seguintes: "É verdade que o sistema AforroNet nao possui multi fator de autenticação, uma prática comum e recomendada."

Além disso, é também verdade que "o sistema AforroNet não possui mecanismos de '*captcha*' para parar ou abrandar ataques automatizados", sendo que "o devia ter". Apesar disso, explica a empresa, "todas as contas do AforroNet tem três possíveis tentativas de login, sendo que ao final das três tentativas erradas a conta fica bloqueada, o que **limita um atacante a fazer um ataque de força bruta** com todas as combinações possíveis".

"No entanto, e dado que o PIN podem ser quaisquer seis dígitos, é possível a um atacante tentar **adivinhar a combinação de dígitos necessária** para entrar na conta AforroNet, isto porque muitas pessoas utilizam PINs como '123456' ou '000000'", explica fonte oficial da empresa.

Para mais, "o **número de contribuinte não é um bom mecanismo de proteção** e serve apenas para identificação de utilizador, uma vez que existem várias fontes onde o nome, email, número de telefone, contribuinte, entre outros, foram capturados e essa informação passou a ser quase pública". Assim, "qualquer atacante que tenha acesso a essa e a outras bases de dados, consegue mapear o nome, email e numero de contribuinte para uma ou várias pessoas que tenham conta AforroNet".

"Apesar de tudo, desde que o PIN escolhido para o utilizador seja aleatório e não seja óbvio como '123456', o **utilizador deve estar protegido** de possíveis entradas na sua conta". A empresa lembra que "os ataques de *brute force* podem não ser tão triviais quanto aparentam", mas que "ataques básicos de *phishing* seriam possíveis e potencialmente mais eficazes".

Verdadeiro