Cotidiano

FALE COM A EDITORA MÁRCIA BRANKI
E-MAILS: cidades@redetribuna.com.br / policia@redetribuna.com.br

Vazamento de senhas expõe empresas e condomínios

Levantamento aponta que cerca de 5,3 mil câmeras de vigilância foram expostas no País, incluindo equipamentos no Espírito Santo

Nicolas Nunes

Cerca de 5,3 mil câmeras de vigilância, em diferentes regiões do Brasil, estavam acessíveis por meio de credenciais digitais vazadas. O levantamento foi divulgado pelo portal UOL.

As imagens mostravam ambientes de empresas, uma unidade de saúde e espaços residenciais. Entre os locais identificados havia equipamentos no Espírito Santo.

Esse tipo de vazamento geralmente acontece por meio do comprometimento de credenciais de acesso, como senhas, explica Lucas Pires, Head de Infraestrutura, Cloud e DevOps da Globalsys.

"Uma das principais formas de ataque envolve programas maliciosos, que infectam computadores e dispositivos para obter senhas armazenadas em navegadores, informações de autenticação e até sessões de acesso", explicou Lucas.

O especialista alerta que os riscos são muito maiores do que ter uma imagem vazada por terceiros.

"O acesso indevido a câmeras de vigilância pode permitir que criminosos acompanhem a rotina de famílias, identifiquem horários em que imóveis ficam vazios, descubram hábitos pessoais e até planejem furtos, roubos e outras atividades criminosas", alertou.

Quando imagens de câmeras de vigilância permitem identificar alguém, elas compreendem dados pessoais protegidos pela Lei Geral de Proteção de Dados (LGPD), destaca Carlos Augusto Pena Leal, advogado especialista em Direito Digital e presidente da Comissão de TI e Direito Digital da OAB-ES.

"As vítimas têm direito de exigir esclarecimentos sobre o ocorrido, quais informações foram comprometidas, quais riscos estão envolvidos e quais providências estão sendo adotadas para impedir novos acessos indevidos", destacou.

Caso o vazamento provoque prejuízos materiais ou morais, é possível pleitear uma indenização judicial contra os responsáveis, conforme as circunstâncias do caso.

Após identificar que foi vítima de um vazamento de dados ou de um ataque virtual, a principal recomendação é substituir, imediatamente, as senhas, manter os equipamentos atualizados e evitar que as câmeras fiquem diretamente acessíveis pela internet.

Quem faz a orientação é Eduardo Pinheiro, especialista em Segurança Digital: "Também é importante ativar a autenticação em dois fatores, e adquirir equipamentos de fabricantes confiáveis", ressalta.



FÁBIO NUNES/AT

LUCAS PIRES diz que vazamentos desse tipo geralmente ocorrem por meio do comprometimento de credenciais de acesso, como senhas

OPINIÕES



"As vítimas têm direito de exigir esclarecimentos sobre quais informações foram comprometidas"

Carlos Augusto Pena Leal, advogado especialista em Direito Digital e presidente da Comissão de TI e Direito Digital da OAB-ES



"É importante ativar a autenticação em dois fatores e ter máquinas de origem confiável"

Eduardo Pinheiro, especialista em segurança digital

SAIBA MAIS

Vazamento de imagens

- **CERCA DE 5,3 MIL** câmeras de vigilância, em diferentes regiões do Brasil, se tornaram acessíveis a terceiros por meio de credenciais vazadas.
- **ENTRE OS** equipamentos estavam câmeras instaladas no Espírito Santo, em empresas, unidades de saúde e espaços residenciais.
- **SENHAS FRACAS** ou repetidas e a ausência de autenticação em dois fatores facilitam o acesso indevido.

Quais os riscos?

- **ALÉM DA** exposição de imagens, o acesso não autorizado permite identificar áreas restritas, movimentações de funcionários, equipamentos e procedimentos de segurança.
- **EM RESIDÊNCIAS**, as gravações podem revelar hábitos familiares e horários de ausência dos moradores.
- **JÁ EM** ambientes públicos, a exposição de imagens de escolas e hospitais pode comprometer a privacidade dos cidadãos e a segurança das instalações.
- **ENTRE OS** possíveis prejuízos estão danos financeiros, reputacionais e operacionais, além de espionagem, extorsão e planejamento de outros crimes.

Direitos das vítimas

- **QUANDO PERMITEM** identificar uma pessoa, as imagens são consideradas dados pessoais protegidos pela Lei Geral de Proteção de Dados (LGPD).
- **AS VÍTIMAS** podem exigir esclarecimentos sobre o incidente, as informações comprometidas, os riscos envolvidos e as medidas adotadas para impedir novos acessos.
- **DEPENDENDO** das circunstâncias, é possível buscar indenização judicial por danos materiais ou morais. A vítima também pode registrar boletim de ocorrência.
- **A DIVULGAÇÃO** de imagens que revelem situações íntimas ou condições de saúde pode representar uma violação particularmente grave da privacidade.

MAGNIFIC



CÂMERAS DE VIGILÂNCIA podem ser uma forma de se obter acesso indevido a informações de áreas restritas, residências e outros locais

Como se prevenir?

- **A PREVENÇÃO** começa pela substituição de senhas padrão de fábrica por combinações fortes e exclusivas.
- **TAMBÉM É** recomendado ativar a autenticação multifator, manter os equipamentos atualizados e evitar que as câmeras fiquem diretamente acessíveis pela internet.
- **EMPRESAS** e órgãos públicos devem restringir permissões de acesso, monitorar atividades suspeitas, revisar credenciais e realizar avaliações periódicas de vulnerabilidades.
- **EM CASO** de vazamento, é importante trocar as senhas, encerrar sessões abertas, comunicar a empresa responsável e preservar provas.

Fonte: Especialistas consultados.