11% dos professores queixa-se de intrusões no ensino à distância. Conheça as regras da cibersegurança

expresso.pt/sociedade/2021-02-23-11-dos-professores-queixa-se-de-intrusoes-no-ensino-a-distancia.-Conheca-as-regras-da-ciberseguranca

Com mais de 1,3 milhões de portugueses ligados em plataformas de ensino à distância, as possibilidades de ataque multiplicaram-se. Não há sistemas informáticos infalíveis, mas talvez tenha chegado a hora de limitar o erro humano. E de pôr termo à partilha de aulas nas redes sociais

Como em muitas modas, "zoom bombing" é uma expressão sonante. O termo “zoom” remete para a plataforma de videoconferências homónima; e “bombing” mais não é que a metáfora usada para ataques que juntam várias visitas indesejadas numa videoconferência – ou numa sala de aula virtual.

A moda que poderá suscitar um sorriso maroto a quem está de fora já deixou milhares de professores portugueses à beira de um ataque de nervos. Segundo um inquérito realizado pelo Centro Nacional de Cibersegurança e a Direção Geral de Educação, 11% dos professores assumiram que viram as suas aulas serem alvo de, pelo menos, um ataque de intrusão virtual entre março e novembro de 2020. Mas os riscos do ensino à distância não se ficam pelo zoom bombing: o mesmo inquérito apurou que 5% dos professores descobriram códigos maliciosos em um ou mais dispositivos, e 3% confirmaram que foram alvo de ataques de partilha não autorizada de vídeos de aulas. Será esta apenas a parte visível de uma ameaça maior?

“É verdade que houve um aumento de ataques durante o ano passado, mas essa tendência parou há três ou quatro meses. Antes dessa diminuição foram apresentadas centenas de queixas nas autoridades. E quase todas estavam relacionadas com ataques a plataformas de videoconferência”, explica fonte ligada à investigação do cibercrime em Portugal, sob anonimato.

Durante a primeira fase de pandemia, muitas escolas não tiveram outra alternativa a não ser acelerar a migração para plataformas de videoconferência. Como todas as mudanças súbitas, houve imprevistos e situações indesejáveis. O que não significa que professores e alunos não tenham aprendido a lição. “No início, as escolas não estavam preparadas. Além disso (os ataques de zoom bombing) eram novidade e possivelmente houve alguns alunos que terão achado piada a fazê-los. Depois passou o fator novidade, e agora já não há tantos ataques deste género. Mas claro que não há sistemas informáticos 100% seguros”, explica Fernanda Ledesma, presidente da Associação Nacional de Professores de Informática (ANPRI).

Para fazer frente às ameaças que pairam na Internet e ao desconhecimento de alunos e professores, o Centro Nacional de Cibersegurança (CNCS) e o Ministério da Educação redigiram um guia prático para facilitar a adoção de regras que minimizam os riscos de ataque. Moodle, Teams (da Microsoft), Classroom (da Google) e Zoom foram algumas das plataformas que mereceram destaque nesse guia. A esta iniciativa juntaram-se ainda seminários na Internet (os webinares) e foi reforçada a ligação às autoridades para facilitar a apresentação de queixas.

Todas estas iniciativas podem ter ajudado a melhorar o cenário, mas há um princípio que norteia a cibersegurança e que nunca poderá ser esquecido: não há sistemas informáticos infalíveis. A este fator acresce outro de especial complexidade: com a migração para a telescola, houve que alargar esse princípio a mais de 1,2 milhões de crianças e adolescentes que passaram a ter aulas à distância – e ainda para os 146 mil professores que, segundo o Pordata, estão atualmente no ativo. Pelo que as percentagens relativas a ataques registados nas aulas à distância registados no inquérito do CNCS e da DGE, ainda que apresentem números diminutos, facilmente podem refletir grupos de centenas ou milhares de pessoas – que dependem dos computadores e da Internet para terem aulas na atualidade.

Acresce a este fator, um outro: não foram só as escolas que passaram a usar a Internet para as atividades diárias. Com mais ou menos restrições, os confinamentos ditados pelos estados de emergência declarados em vários países levaram uma parte considerável da população mundial enveredar por atividades à distância, suportadas pela Internet. E os cibercriminosos estão atentos a essa tendência. O que teve um efeito direto no número de ameaças detetadas.

Segundo dados compilados pelo CNCS, o número de incidentes de cibersegurança detetados passou de 754 para 1418 de 2019 para 2020. Nesta cifra, destaca-se o número de incidentes relacionados com phishing, um método de ataque em que um cibercriminoso tenta ludibriar a vítima com um endereço falso ou um download com um código malicioso para infetar e ganhar acesso a um ou mais computadores. Os dados do

CNCS apuram que que foram contabilizados 236 incidentes de phishing em 2019, e que em 2020 essa contabilidade foi fixada em 613 incidentes. No total, os incidentes de phishing representaram 43% do total de incidentes de cibersegurança trabalhados pelo CNCS em 2020.

O CNCS contabiliza estes incidentes tendo em conta o impacto que poderão ter em qualquer internauta. Ainda que estes números possam ajudar a descrever a realidade em que alunos e professores portugueses se deparam na atualidade, não é feito um estudo especializado nas ameaças direcionadas para o ensino à distância. “Um incidente pode produzir uma, várias ou nenhuma vítima. Quando tomamos conhecimento destes incidentes, tentamos bloqueá-los, avisando as autoridades ou as entidades que gerem os servidores usados para disseminar estes incidentes”, explica Lino Santos, coordenador do CNCS.

Os dados compilados pela Kaspersky também confirmam que os cibercriminosos têm estado atentos à chegada de um grande número de novas vítimas à Internet. Aquela empresa de cibersegurança estima que o número de vítimas que foram atacadas através de sistemas usados no ensino à distância terá registado um aumento de 60% do primeiro para o segundo semestre de 2020. No total, os ataques levados a cabo através de plataformas de videoconferência terão feito mais de 200 mil vítimas em todo o mundo durante o segundo semestre do ano passado.

Além de organizados numa lógica empresarial que prevê a divisão de tarefas e a transação de recursos e ferramentas, os cibercriminosos seguem de perto a lei da oferta e da procura. E é essa lógica que leva a concluir que o aumento de campanhas maliciosas estará diretamente ligado à grande fatia da população que está em teletrabalho e aulas suportadas pela Internet, ou que faz compras na Internet com regularidade.

Lino Santos acrescenta ainda que o facto de o CNCS ser cada vez mais conhecido da população também ter ajudado a recolher mais queixas e denúncias de incidentes de cibersegurança. Sobre o ensino à distância, recorda a diferença entre aulas suportadas pela Internet e a Internet em geral, que existe fora das aulas: “O ensino à distância tem um ambiente relativamente controlado, mas se os alunos começarem a navegar na Internet ou precisarem de usar outras aplicações acabam por sair desse ambiente controlado”, explica.

Mesmo num ambiente controlado, os riscos existem. Nas aulas, como em qualquer atividade na Internet, o princípio da desconfiança deverá estar sempre presente – e se não for o princípio da desconfiança, pelo menos, convém não seguir o facilitismo que leva a descarregar qualquer aplicação que um colega envia sem ter em conta a proveniência, ou não clicar em anúncios que oferecem telemóveis topos de gama sem razão plausível para isso.

Rui Duro, gestor da Check Point em Portugal, também confirma que a deteção de vulnerabilidades e incidentes foi maior na primeira fase da pandemia, ainda durante o primeiro trimestre de 2020. Depois dessa primeira vaga de confinamentos, houve um

esforço generalizado para levar a cabo atualizações de segurança e usar ferramentas mais seguras.

“Para as crianças que já tinham experiência, o risco não aumentou, porque já sabiam usar a Internet. Mas depois temos um grupo de milhares de crianças que não costumavam usar a Internet, mas que agora têm de aceder todos os dias a plataformas de ensino. São potenciais vítimas de ataque, mesmo que esses ataques não estejam diretamente relacionados com a telescola”, explica o responsável da Check Point.

A ideia de decréscimo de incidentes relacionados com as aulas à distância não é totalmente consensual na comunidade da cibersegurança. “Este segundo confinamento e consequente regresso às aulas à distância, bem como ao teletrabalho, colocou-nos novamente na mira dos ciberataques, uma vez que muitas das vulnerabilidades de segurança digital verificadas no primeiro confinamento mantêm-se. Por exemplo, continuam a existir notícias de aulas invadidas por pessoas externas às escolas”, refere Bruno Castro, diretor da empresa de segurança eletrónica VisioWare, por e-mail.

Uma coisa é certa: a inexperiência de muitas crianças que acabam de chegar às aulas à distâncoia é apenas uma das vertentes em que se enquadram todas as vulnerabilidades que costumam ser apelidadas de “erro humano”. Com o erro humano, até as plataformas com a melhor arquitetura e encriptação podem acabar por sucumbir. Precisamente porque as proteções são superadas pelo facto de haver um ou mais utilizadores, intencional ou inadvertidamente, ações de risco. “Já tive conhecimento de aulas lecionadas a crianças que permitiam acesso às plataformas de videoconferência em que decorrem as aulas sem qualquer password”, refere António Ribeiro, diretor de cibersegurança da Claranet, apontando um exemplo de vulnerabilidade motivada por humanos e questionando se houve mesmo um decréscimo nos incidentes nos últimos meses.

É também devido ao fator humano que começaram a ser partilhados em redes sociais e plataformas de mensagens excertos de vídeos e áudios retirados das aulas à distância. “Não me parece que seja legal, e são comportamentos que têm vindo a ser sancionados”, refere Filinto Lima, presidente da Associação Nacional de Diretores de Agrupamentos de Escolas Públicas (ANDAEP). “Esta partilha de vídeos ainda não é uma prática generalizada, mas os professores e encarregados de educação têm de alertar para a responsabilidade cívica dos alunos”, acrescenta o dirigente da ANDAEP, defendendo a responsabilização dos pais como forma de prevenir as partilhas indevidas.

Até pode acontecer que o ensino à distância perca expressão depois da pandemia, mas há lições que não podem ser ignoradas nos tempos mais próximos. Até porque a Internet vai continuar a ser usada por quase todos, mesmo fora das aulas. “Os professores têm de integrar nas aulas e atividades didáticas dedicadas à cidadania matérias que estão relacionadas com o ambiente digital”, conclui António Ribeiro.

Conselhos de segurança:

Para alunos:

- Evitar a exposição desnecessária de dados pessoais, imagens ou de detalhes da vida pessoal.

- Manter sistemas operativos e diferentes aplicações devidamente atualizadas, para evitar o número de vulnerabilidades que podem ser exploradas.

- Não esquecer de alterar a password que vem de origem com o router para uma password de conhecimento estritamente pessoal ou familiar.

- Usar sistemas de proteção (geralmente conhecidos como antivírus) nos computadores usados para aceder às aulas

- Usar uma password diferente para cada sessão ou plataforma usada durantes as aulas

Para professores:

- As sessões de aulas em videoconferência devem ter sempre password de acesso e sala de espera até ser garantida a autorização para entrar.

- Não esquecer de fazer atualizações de sistemas operativos e aplicações nos computadores usados para lecionar as aulas em videoconferência.

- Usar sistemas de proteção nos computadores usados para lecionar as aulas

- Definição de regras de cibersegurança. “As escolas vão ter de adotar os guias de implementação do teletrabalho e definir junto de alunos e pais as regras que têm de ser aplicadas”, sugere Rui Duro

- Especial cuidado nas ferramentas de partilha de informação e conteúdos com os alunos – pois é um dos vetores de ataque explorado pelos hackers, que tentam intrometer-se em links, repositórios de dados alojados na Internet ou endereços de e-mail para contagiarem novas vítimas

Para encarregados de educação:

- Muitospais e encarregados de educação partem em desvantagem em relação às crianças pelo facto de não serem tão versados no uso das tecnologias e de não terem o tempo disponível ou o engenho para descobrir falhas e modos de uso das tecnologias menos previsíveis. Pelo que antes de aplicar regras e princípios às crianças, convém procurar alguma informação junto de fontes credíveis.

- Pode ser usado software de controlo parental, que permite saber o que faz um menor com o computador quando está ligado à Internet – mas com uma lógica construtiva. “O software de controlo parental deve ser usado, mas não de forma punitiva (no caso de ser detetada uma atividade irregular). Além disso, convém não esquecer que os adolescentes encontram forma de contornar este tipo de software”, explica António Ribeiro.

- Manter uma atitude educativa, que mostra benefícios e também riscos da Internet para os novos