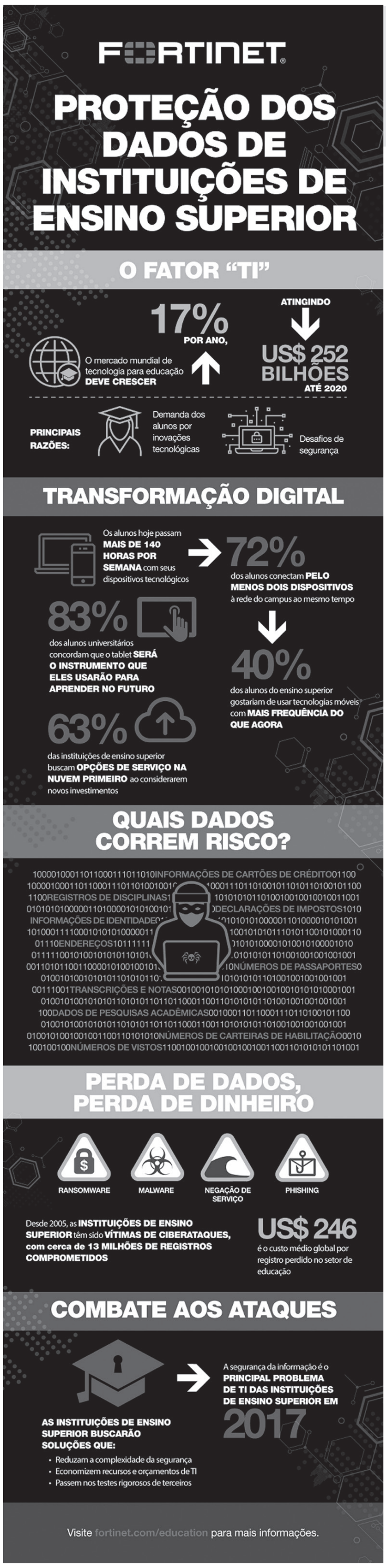

Instituições de ensino superior são alvos de ciberataques

A proliferação da conectividade em toda a rede global teve uma série de impactos positivos nas instituições de ensino superior graças aos avanços tecnológicos e ao crescente número de dispositivos conectados. De serviços da nuvem à tecnologia de Internet das Coisas (IoT), alunos e professores agora podem ficar conectados, mesmo fora da sala de aula, melhorando seu sistema de aprendizagem e suas pesquisas

Susan Biddle (*)

Porém, esta troca de informações contínua também resultou em aumento no número de cibercriminosos que usam as instituições educacionais como alvo. Todas as informações trocadas, sejam elas dados pessoais de um aluno ou dados de pesquisas acadêmicas, devem ser protegidas para preservar a reputação institucional.

As faculdades e universidades geralmente têm ambientes com grande fluxo de pessoas e são altamente colaborativas. Elas exigem acesso a vários recursos e publicações online para a realização de pesquisas, trabalhos acadêmicos ou preparação de aulas, além do acesso a vários aplicativos e programas para gravar, apresentar e compartilhar informações. Sem contar que, dependendo do instituto ou do departamento, a importância de acessar diferentes aplicativos e recursos varia significativamente.

Além de ajudar a atender às necessidades acadêmicas, as equipes de TI de instituições de ensino superior também devem construir uma rede sem fio (WLAN) com capacidade de conectar todos os dispositivos que os alunos usam diariamente, como smart TVs, impressoras sem fio, dispositivos móveis e muito mais.

A construção de uma rede sem fio com a largura de banda e a capacidade de lidar com tráfego tão intenso e prioridades variáveis é um desafio por si só. Não é difícil ver faculdades e universidades implementando centenas ou até milhares de pontos de acesso em seu campus para oferecer cobertura Wi-Fi ininterrupta.

Este desafio de infraestrutura é ainda mais complicado quando se trata de ameaças de segurança agora associadas a redes abertas em instituições de ensino superior. Hoje, as equipes de TI de universidades precisam construir infraestruturas de WLAN que oferecem conectividade forte, com poucas restrições

e tempo de inatividade mínimo, além de protegerem os usuários e os dados das ameaças atuais em constante evolução.

As faculdades e universidades se tornaram alvos de grande valor para os cibercriminosos por causa dos tipos de dados que elas armazenam, que não são apenas informações sobre os alunos matriculados, pois incluem informações de saúde, financeiras e pessoais de professores, funcionários, administradores e até mesmo candidatos. Desde 2005, as instituições de ensino superior foram vítimas de 539 ataques, resultando em 13 milhões de registros comprometidos. Outras instituições de ensino também correm risco de invasões, pois armazenam dados de propriedade intelectual de pesquisas originais realizadas em laboratórios ou outros centros de pesquisa.

As arquiteturas seguras levam em conta os desafios de conectividade que atingem as universidades atualmente, como cobertura, confiabilidade e capacidade de fornecer acesso a um grande número de dispositivos pessoais, além de oferecerem soluções avançadas de cibersegurança. As instituições educacionais da América Latina já começaram a implementar com sucesso esse tipo de solução de acesso seguro, como a Escola San Ignacio de Loyola na Colômbia e o centro educacional IFB Certus no Peru.

O uso de tecnologia em campus universitário continua aumentando à medida que os alunos se tornam mais dependentes de dispositivos e aplicativos conectados em suas vidas acadêmicas e pessoais. Ao mesmo tempo, as universidades enfrentam ciberataques mais frequentes e sofisticados de criminosos que procuram dados pessoais valiosos. As universidades têm que integrar seus protocolos de acesso e segurança de rede para fornecer escalabilidade e visibilidade e atender às necessidades dos alunos, protegendo-se das ciberameaças atuais e futuras.

Veja números adicionais no infográfico ao lado.

(*) É Diretora de Marketing Sênior para o setor de educação da Fortinet.

Vazamento de dados é principal falha de 65,8% dos aplicativos web, diz pesquisa

Apesar dos investimentos em segurança de dados se mostrarem cruciais para as empresas, como evidenciado pelos recentes cibertaques que sequestraram informações confidenciais de usuários ao redor mundo, as aplicações não são mais seguras hoje do que eram há uma década. É o que revela estudo produzido pela Veracode, líder mundial em segurança de softwares e recentemente adquirida pela CA Technologies, com 1.400 empresas avaliadas. Pelo menos uma falha foi encontrada nos testes iniciais de 77% dos apps analisados na pesquisa e 25% dos sites contém pelo menos uma vulnerabilidade grave.

O estudo ainda mostra que houve uma redução no índice de falhas em nove, das dez principais, vulnerabilidades dos aplicativos. No entanto, os números ainda devem preocupar companhias que utilizam algum serviço baseado em apps. A pesquisa identificou que 12% de todas as aplicações analisadas tinham ao menos uma falha grave.

"Ao longo de um ano, foram quase 250 bilhões de linhas de código analisadas. Vimos que os clientes têm priorizado a correção das falhas mais graves, mas mais de 50% das correções levaram mais de 90 dias para acontecer. Isso preocupa, porque a maioria dos ataques acontecem poucos dias depois da descoberta de uma falha", comenta Denyson Machado, vice-presidente de segurança para América Latina na CA Technologies.

Entre as dez principais falhas registradas, a primeira está relacionada a um dos maiores medos das corporações: proteção de dados. De acordo com a pesquisa da Veracode, falhas que geram vazamento de informação caíram 7% e hoje acontecem em 65,8% dos apps (em 2016, 72,1% dos apps apresentavam esse tipo de falha). Problemas de criptografia, a segunda falha mais recorrente, também tiveram redução – de 65,9% para 61,5% -, mas ainda ocupam a segunda posição das falhas mais frequentes. Fechando o top 3 está a qualidade do código – caindo de 61,7% para 56,2% dos apps testados.

Segundo os especialistas da CA Technologies, a queda no percentual das principais falhas não é resultado de uma melhora nos apps e nem deve ser tido como resultado de uma maior adoção de testes de código no processo de desenvolvimento. "Os dados mostram que houve, na verdade, uma pulverização das falhas, com o aumento de outros tipos de problemas na produção dos apps", comenta Machado.

TESTES CONTÍNUOS

Cerca de 70% das aplicações analisadas pela primeira vez não tiveram sucesso em passar por testes de OWASP (Projeto Aberto de Segurança em Aplicações Web), comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web.

"A pressa de entregar o produto ao mercado gera problemas durante o desenvolvimento do código e os aplicativos são entregues com falhas de segurança. Os testes contínuos existem e estão disponíveis para que o desenvolvedor não cometa o erro de entregar um produto mal-acabado", afirma João Fábio Valentin, VP de Solution Sales para DevOps da CA Technologies para América Latina.

Com resolução de problemas entre as fases de pré-produção e produção, a tendência de DevSecOps é confirmada. Dos servidores web analisados, 25% continham ao menos uma vulnerabilidade crítica. Nesse caso, mesmo que o desenvolvedor não escreva nenhum código vulnerável, a insegurança do servidor em si compromete a segurança da aplicação. Além disso, mais de 18% das versões dos servidores analisados tinham mais de 10 anos de lançamento.

Apesar de 71%* das organizações brasileiras apontarem o uso de teste contínuo como essencial ou importante, somente 22% adotam esta prática de última geração, que permite executar testes com antecedência e com frequência, de forma automática e constante, no desenvolvimento de software e aplicações.

--

* De acordo com o levantamento "Testes Contínuos como um elemento fundamental da empresa digital"

News @TI

Startup lança software para gestão de marcas e patentes

@O Ilupi, startup especializada em gestão online de marcas e patentes, lança software focado na gestão e monitoramento de ativos na área de propriedade intelectual. Com o Ilupi, startups e empresas pequeno porte terão uma alternativa digital, transparente e econômica. Os serviços prestados incluem desde o registro de marcas, patentes e softwares junto ao Instituto Nacional de Propriedade Industrial (INPI) até a vigilância do que foi registrado, recebendo atualizações automáticas de seus processos e de seus concorrentes. Além disso, os usuários contarão com o apoio de especialistas para atender as demandas do próprio INPI, tudo em uma única plataforma 100% online, que proporciona agilidade nos processos, diminuição da burocracia e preços mais acessíveis (www.ilupi.com.br).

Empresas & Negócios
netjen@netjen.com.br
Para veiculação de seus Balanços, Atas, Editais e Leilões neste jornal, consulte sua agência de confiança, ou ligue para
TEL: 3106-4171