LIVRO BRANCO

PORTAS ABERTAS

UM ESTUDO REVELA QUE AS IMPRESSORAS SÃO VULNERÁVEIS A ATAQUES INFORMÁTICOS

Enquanto as equipas de TI se concentram noutros pontos finais, a segurança das impressoras empresariais é negligenciada

As impressoras são alvos fáceis: Demasiadas impressoras ligadas à rede não têm quaisquer restrições e não estão devidamente protegidas.

A ameaça é real e não deve ser ignorada. As impressoras de classe empresarial evoluíram para poderosos dispositivos ligados em rede que apresentam as mesmas vulnerabilidades de qualquer outro ponto final na sua rede. Normalmente, estes pontos de entrada não estão protegidos e permitem a ocorrência de ataques informáticos; estes também podem ser uma porta de entrada para os *hackers* acederem aos dados financeiros e privados da sua empresa, gerando consequências empresariais reais muito graves.

Um inquérito da Spiceworks, realizado recentemente a mais de 300 responsáveis pelas TI, revelou que apenas 16% dos inquiridos considera que as impressoras constituem um risco elevado de ameaça à segurança/violação da segurança, um valor significativamente inferior ao dos desktops/portáteis e dispositivos móveis.[1] Esta perceção afetou o modo como as equipas de TI encaram a segurança da rede. Não obstante o facto de três em cada cinco organizações disporem de práticas de segurança vigentes relativamente a impressoras, esta percentagem é muito inferior à das relacionadas com outros pontos finais, o que deixa as impressoras vulneráveis apesar de haver soluções fáceis para proteger este ponto de entrada específico.

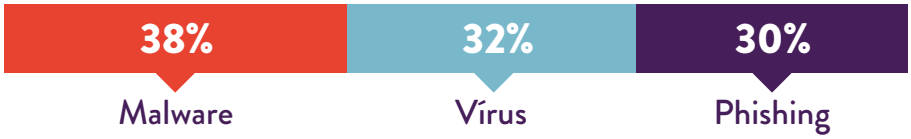
Este livro branco apresenta dados sobre a segurança de impressoras baseados no inquérito da Spiceworks, o impacto das violações de segurança e algumas das funcionalidades de segurança incorporadas em impressoras concebidas para as proteger de ataques informáticos.

APENAS 16% DOS INQUIRIDOS CONSIDERAM QUE AS IMPRESSORAS CONSTITUEM UM RISCO ELEVADO DE AMEAÇA À SEGURANÇA/VIOLAÇÃO DA SEGURANÇA.[1]

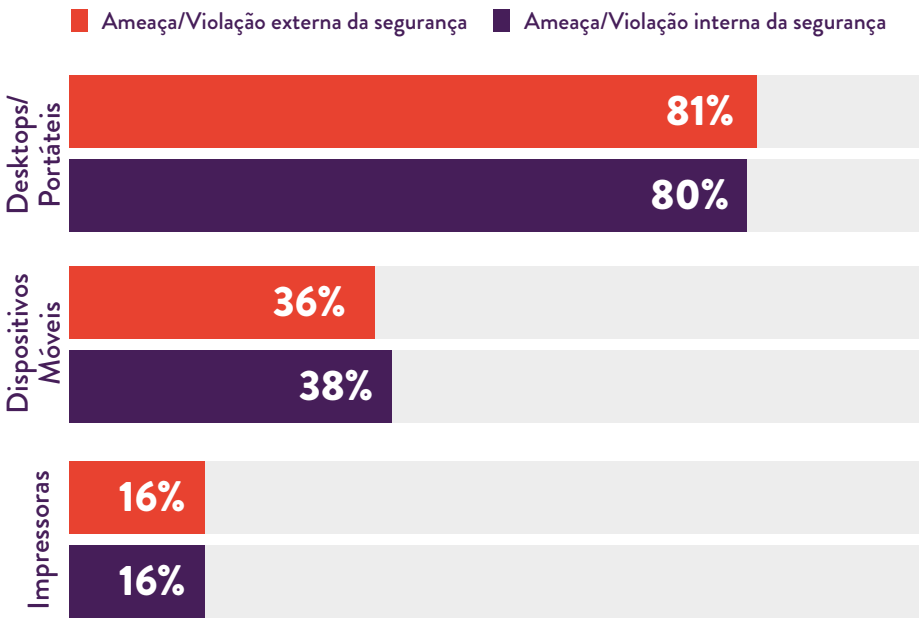
PORTAS DE ENTRADA PARA ATAQUES

No inquérito da Spiceworks, 74% dos inquiridos (líquido) afirmaram que a sua organização sofreu algum tipo de ameaça ou violação externa da segurança de TI no último ano. E 70% (líquido) sofreram uma ameaça ou violação interna da segurança de TI, normalmente devido a erros de utilizadores, à utilização de dispositivos pessoais para fins profissionais ou a funcionários que recorrem a uma rede doméstica ou pública para fins profissionais.[1]

PRINCIPAIS AMEAÇAS/VIOLAÇÕES EXTERNAS DA SEGURANÇA DE TI SOFRIDAS



As principais ameaças ocorrem principalmente através desktops e portáteis, ao passo que outras ocorrem através de dispositivos móveis e impressoras.[1] (Os 16% que ocorrem através de impressoras são notoriamente mais elevados do que os 4% determinados num estudo semelhante ao da Spiceworks relativo a 2014.) É também possível que o número de ataques ocorridos através de impressoras seja subestimado, já que estas não são tão rigorosamente monitorizadas como os PCs e os dispositivos móveis.



ESTAMOS A IGNORAR AS NOSSAS IMPRESSORAS

Independentemente da situação, o inquérito da Spiceworks deixa bem claro que a segurança das impressoras é frequentemente uma prioridade secundária.

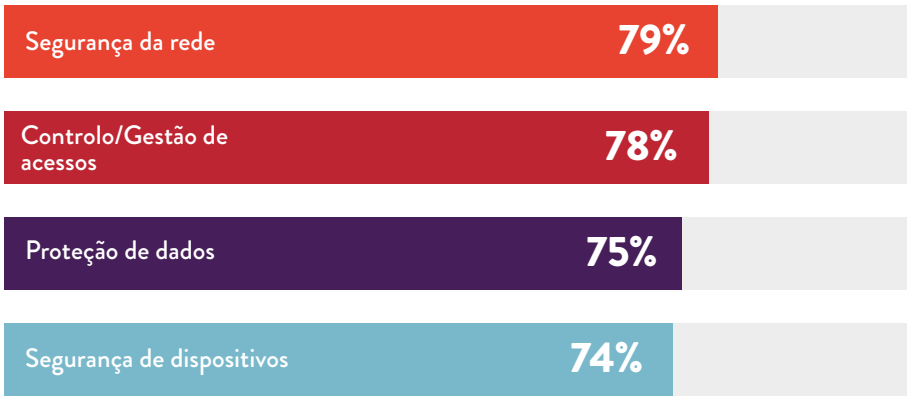
As organizações estão perfeitamente cientes da importância da segurança relativamente a redes, pontos finais e dados. Na realidade, mais de três quartos dos inquiridos recorrem às seguintes formas de segurança: segurança da rede, controlo/gestão do acesso, proteção de dados, segurança dos pontos finais ou uma combinação de todos estes.[1]

No entanto, estas soluções são implementadas com menos frequência em impressoras. Embora 83% dos inquiridos usem a segurança da rede em desktops/portáteis e 55% em dispositivos móveis, apenas 41% usam-na em impressoras.[1]

A disparidade é ainda maior no caso da segurança dos pontos finais:

Além disso, nem um terço (28%) dos inquiridos implementam certificados de segurança para impressoras em oposição a 79% para PCs e 54% para dispositivos móveis.[1]

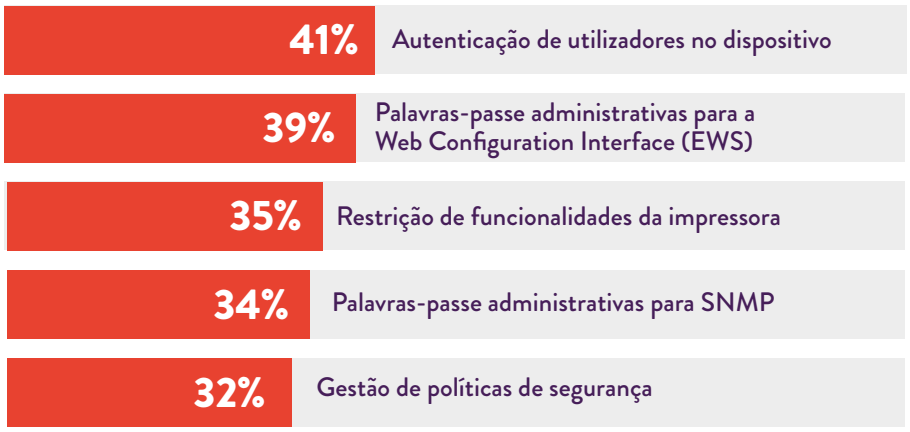
PRINCIPAIS PRÁTICAS DE SEGURANÇA PARA PONTOS FINAIS



De entre as proteções utilizadas em dispositivos de ponto final gerais, as medidas de segurança mais utilizadas para impressoras foram a segurança dos documentos, a segurança da rede e o controlo do acesso, mas menos de metade dos inquiridos afirmou que as suas organizações não usam nenhuma destas medidas nas suas impressoras.[1]

Algumas empresas dispõem de medidas de segurança específicas para impressoras, mas, mesmo neste caso, as práticas são demasiado díspares. Mais de 40% das organizações implementaram autenticação do utilizador, e menos de 40% utilizavam palavras-passe de administrador para a Web Configuration Interface (EWS).[1] Para uma sólida defesa e proteção, cada organização deveria combinar todas estas abordagens e outras mais.

PRINCIPAIS PRÁTICAS DE SEGURANÇA ESPECÍFICAS PARA IMPRESSORAS



No que diz respeito à conformidade dos pontos finais e às práticas de auditoria, os controlos de segurança das impressoras são negligenciados em praticamente todos os demais pontos finais. Aproximadamente 90% das organizações não dispõem de uma política de segurança de informações implementada, embora, normalmente, tais políticas não abranjam impressoras. Por exemplo, não obstante o facto de 57% dos inquiridos terem afirmado que implementaram defesas contra malware nos seus PCs, apenas 17% tinham implementado tais defesas nas suas impressoras.[1]

APROXIMADAMENTE 9 EM CADA 10 PROFISSIONAIS DE TI AFIRMAM QUE A SUA ORGANIZAÇÃO DISPÕE DE UMA POLÍTICA PARA A SEGURANÇA DE INFORMAÇÕES PELOS SEGUINTES MOTIVOS:

É mais que óbvio que as organizações não estão a dar a devida importância à segurança das impressoras, embora devam fazê-lo.

"Muitas impressoras ainda têm as palavras-passe predefinidas, ou não têm sequer qualquer palavra-passe configurada, ou dez impressoras chegam a utilizar a mesma palavra-passe", afirmou Michael Howard (consultor-chefe de segurança para a HP) à publicação Computerworld em junho passado. "Uma impressora sem proteção de palavra-passe é uma mina de ouro para qualquer *hacker*. Uma das violações com que frequentemente nos deparamos é um ataque tipo "man-in-the-middle" (o homem do meio), durante o qual o *hacker* assume o controlo da impressora e encaminha documentos recebidos para um computador portátil antes de serem impressos. O *hacker* consegue ver tudo o que o Presidente do Conselho de Administração está a imprimir."[2]

O POTENCIAL IMPACTO DAS INTRUSÕES EM IMPRESSORAS

Segundo Bogdan Botezatu, um analista sénior de ataques informáticos da Bitdefender, as impressoras constituem uma potencial considerável falha de segurança. "Recebemos um volume considerável de telemetria nos nossos laboratórios de avaliação de vulnerabilidades. O router já não é o dispositivo mais vulnerável na Internet. A impressora tem agora essa distinção."[3]

Esta vulnerabilidade pode ter impactos profundos numa empresa. Basta haver uma única impressora desprotegida para deixar toda a sua rede de dispositivos conectados vulnerável a ataques, permitindo aos *hacker*s espiar os seus dispositivos ligados em rede e comprometendo a segurança de toda a sua rede.

1. Aumento do número de chamadas ao suporte técnico e aumento do tempo de suporte

2. Redução da produtividade/ eficiência

3. Aumento do tempo de indisponibilidade do sistema

4. Aumento do tempo despendido em chamadas de suporte

5. Reforço da aplicação das políticas do utilizador final

Todos nós já sabemos as consequências das violações da segurança. No inquérito da Spiceworks, os inquiridos afirmaram que os cinco principais impactos de uma violação são:[1]

Mas uma violação da impressora pode ser muito mais grave, sobretudo se utilizar uma impressora multifunções capaz de armazenar dados impressos de forma eletrónica. Os trabalhos de impressão armazenados na cache da impressora permitem aos *hackers* aceder a informações pessoais ou comerciais confidenciais.

O que é ainda mais preocupante é o facto de os *hackers* poderem aceder, de uma forma mais vasta, à rede da empresa através de uma impressora desprotegida para roubar dados, como os números da Segurança Social, informações financeiras ou memorandos e documentos internos. As informações roubadas não só poderão prejudicar individualmente os funcionários, como também poderão ser aproveitadas pela concorrência ou para manchar seriamente a reputação de uma empresa.

A SOLUÇÃO FÁCIL: FUNCIONALIDADES DE SEGURANÇA INCORPORADAS

É mais que óbvio que as empresas precisam de dar a devida importância à segurança, até mesmo no que diz respeito às suas impressoras. Algumas das atuais modernas impressoras de nível empresarial incorporam funcionalidades de segurança de fácil utilização que protegem as mesmas de ameaças e de ataques. Estas incluem:

- Deteção, proteção e resolução automáticas de ataques
- Controlo da utilização para impedir a utilização não autorizada
- Opções simples de início de sessão, como PIN ou smartcards
- Um leitor de cartões de proximidade que permite aos utilizadores autenticarem-se com rapidez e imprimir em segurança numa impressora ao utilizar o seu crachá de identificação
- Proteção da impressão encriptada para documentos confidenciais

Estude as proteções de segurança integradas antes de adquirir a sua próxima impressora, independentemente de ser de secretária ou multifunções, e não se esqueça de as ativar. Com funcionalidades simples e específicas para impressoras como estas, o risco de vulnerabilidade para as suas impressoras é praticamente nulo; afinal, com a Internet das Coisas, existem vários pontos de acesso com que se preocupar, e **as suas impressoras não precisam de ser mais um motivo de preocupação.**

ESTÁ À PROCURA DE IMPRESSORAS MAIS SEGURAS?

SAIBA MAIS ›

Fontes:

[1] Inquérito da Spiceworks realizada, em nome da HP, a 309 responsáveis pelas TI nas regiões da América do Norte, Europa, Médio Oriente e África, e Ásia-Pacífico (novembro de 2016).

[2] "Printer Security: Is your company's data really safe?", *Computerworld* (1 de junho de 2016). http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet", *The Register* (8 de setembro de 2016). http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/