Manter um ambiente de impressão seguro

Terceiro relatório da série Transformação Digital realizado pela Brother

Relatório
Extraído de uma pesquisa de mercado

brother.pt

Obstáculos ao investimento na segurança da impressão

Devido à crescente ameaça de ataques informáticos e falhas de segurança que põem em risco a confidencialidade, muitas empresas estão cada vez mais conscientes da necessidade de proteger os seus sistemas de TI.

Gerir a segurança do parque tecnológico é um desafio que necessita ser abordado de forma global. E as impressoras e scanners necessitam ser tão seguros como o resto dos equipamentos de TI já que, se não lhes é dada a devida atenção, corre-se o risco de que estejam a abrir uma porta aos hackers, fácil de atravessar, para entrar na organização. As empresas, estão cada vez mais conscientes da importância deste facto: 72% asseguram que é fundamental que as suas impressoras e scanners sejam seguros, e inclusivamente isto é mais importante para os que lidam com dados sensíveis em setores como Serviços Profissionais (82%) e Saúde (81%).

No entanto, um terço das companhias ainda não reconhece a sua importância. E quase metade dos entrevistados pensa que a sua empresa não investiu o suficiente na segurança do hardware de impressão.

Se as empresas entendem a necessidade de investir na segurança dos seus equipamentos de impressão, porque não o fazem?

A nossa investigação mostra duas razões principais:

Responsabilidades pouco definidas sobre a segurança das impressoras

Falta de conhecimentos sobre as regras e ameaças de segurança

Este relatório foi pensado para ajudar diretores e decisores empresariais a conhecer a importância da segurança no ambiente de impressão e a forma de implementar soluções de impressão seguras. Faz parte de uma série de relatórios mais amplos que pretende ajudar a entender qual é a melhor forma de utilizar as tecnologias digitais. Baseámos as conclusões em pesquisas de mercado realizadas entre diretores e decisores de uma ampla variedade de pequenas, médias e grandes empresas da região EMEA.

Este documento faz parte de uma série de quatro relatórios, cada um focado num dos seguintes temas:

- Fluxos de trabalho digitais
- Implementar a solução adequada para a empresa
- Segurança
- Sustentabilidade

Quem é o responsável pela segurança das impressoras?

Frequentemente surgem dúvidas sobre quem é a pessoa responsável pela segurança dos equipamentos de impressão. Quase metade das empresas da Europa Ocidental **(44%)** asseguram que não está claro quem é o responsável de segurança na impressão dentro da sua organização. E como não se sabe quem é responsável por esta área, é muito provável que a tomada de decisões e a implementação de medidas de segurança para a impressão sofram, deixando a empresa numa situação vulnerável.

Normalmente não é designado um responsável para a segurança da impressão porque não se reconhece tradicionalmente um equipamento de impressão como um 'ponto débil', ao contrário de outros dispositivos como os portáteis. Embora a nossa investigação demonstre que os decisores estão a começar a dar conta de que a segurança neste ambiente é vital, as funções nas empresas não parecem refleti-lo ainda.

As pequenas e médias empresas são especialmente vulneráveis a esta falta de responsabilidade, já que muitas vezes é um pequeno número de colaboradores que cuida de todo o hardware e software da empresa. Se os profissionais de TI não estão conscientes dos riscos da segurança na impressão, para eles será uma prioridade baixa.

No entanto, todos os trabalhadores de uma empresa têm uma parte de responsabilidade na hora de garantir que a informação sensível se mantém segura.

Enquanto os especialistas em tecnologia se encarregam da segurança dos dispositivos em si, os colaboradores têm a responsabilidade de manter a segurança dos próprios dados.

A segurança dos dados inclui um amplo leque de ameaças, entre as quais se encontram:

- Acesso não autorizado aos documentos impressos
- Esquecer de fechar a sessão depois de imprimir documentos confidenciais
- Falta de rastreabilidade sobre quem acedeu a que documentos na impressora

Quase 9 em cada 10 empresas experienciaram algum incidente de segurança relacionado com a impressão…

... e sete em cada dez **(72%)** asseguram que a segurança dos dados é uma ameaça maior que a segurança do dispositivo. No entanto, atualmente menos de um terço das empresas dizem estar 'muito seguras' de que a sua infraestrutura de impressão inclui medidas de segurança suficientes, enquanto **53%** pensam que têm a segurança adequada nos seus equipamentos de hardware.

A maioria das empresas **(64%)** também afirma que garantir a segurança dos seus dados é uma prioridade. Isto é visto como um desafio importante e pode ser um entrave para um rendimento eficiente.

Atualmente, quase metade das empresas **(48%)** dizem ter poucos ou nenhuns processos que as permitam saber com certeza, quem imprime ou recolhe os trabalhos impressos. Como tal, não é surpreendente que quase nove em cada dez **(86%)** afirmem ter tido incidentes de segurança relacionados com a impressão: documentos confidenciais que foram deixados sem supervisão na impressora, impressões que não foram recolhidas ou colaboradores que recolhem documentos confidenciais que não são seus.

Como resultado, a maioria das empresas **(64%)** estão a começar a implementar medidas para abordar este tipo de problemas de segurança, restringindo o acesso a certos equipamentos ou introduzindo códigos PIN ou cartões de identificação para que os trabalhos de impressão sejam libertados apenas pela pessoa adequada.

São passos no bom caminho. Nos próximos anos será importante que, as empresas que não os têm, introduzam processos mais seguros; e as que já o fazem, mantenham e melhorem a sua responsabilidade e as suas auditorias internas.

Há 3 objetivos principais para conseguir uma segurança real da informação, resumidos no acrónimo CIA, que cobrem tanto a segurança do equipamento como a dos dados:

Confidencialidade

Proteger os dados confidenciais da empresa para garantir que apenas são partilhados com o seu destinatário. Para tal é fundamental ter medidas de autentificação e autorização que requerem aos utilizadores a verificação da sua identidade e comprovem que têm permissão para fazer o que estão a tentar fazer, antes de que seja libertado qualquer documento impresso.

Integridade

Assegurar que o firmware do equipamento é seguro e resistente a qualquer possível ataque ou ameaça externa.

Acessibilidade

Assegurar que o equipamento está a funcionar e acessível aos utilizadores autorizados para realizar as suas tarefas.

A falta de conhecimento leva a práticas de segurança pouco apropriadas

Menos de um terço **(32%)** dos decisores de TI das empresas dizem ter um conhecimento avançado em segurança tecnológica e os seus potenciais riscos. Se não têm informação suficiente sobre as ameaças, então as empresas continuarão a ter problemas para colocar em marcha as medidas adequadas para se protegerem. Nas pequenas e médias empresas, o papel do decisor cobre normalmente várias e diversificadas áreas tecnológicas, sendo por isso compreensível que não sejam especialistas na segurança, específica, do ambiente de impressão.

A responsabilidade, muitas vezes, não é entendida. Mais de metade **(51%)** das empresas queixam-se de que há demasiado vocabulário novo relacionado com a segurança de impressão.

No que diz respeito aos standards de segurança, quase **60%** das empresas diz conhecê-los bem.

Com tudo isto, é pouco provável que os decisores conheçam bem ou saibam que fornecedores de tecnologia de impressão podem cobrir melhor as suas necessidades de segurança. Por isso, não é surpresa que as empresas procurem marcas que 'conhecem' para os seus equipamentos de impressão, sem se preocupar em saber realmente que medidas de segurança incorporam ou não.

É responsabilidade dos fornecedores de impressão ajudar as empresas a entender as normas sobre segurança relativas à impressão e assegurar que cada uma escolhe a melhor solução para as suas necessidades.

A visão da Brother

Dada a complexa natureza do panorama de segurança da impressão, a Brother oferece 7 recomendações chave que podem ajudar as empresas a protegerem-se das enormes implicações financeiras, legais e de reputação de uma perda de dados.

Implicar o comité de direção

O aumento de ciberataques e falhas de segurança, combinada com os requerimentos do Regulamento Geral de Proteção de Dados (RGPD), implica que a segurança da impressão necessita ir mais além do domínio do departamento de tecnologia. Deve ser considerada de maneira estratégica no comité de direção, com a participação do responsável de informática (CIO) e do responsável de segurança (CISO).

Levar a cabo uma auditoria exaustiva

Para as empresas é fundamental descobrir qualquer potencial vulnerabilidade relacionada com a segurança da impressão e assegurarem-se de que este ambiente está incluído nas auditorias regulares de segurança. Isto é especialmente importante se a empresa tem uma mistura de dispositivos novos e antigos. Quanto aos Serviços de Gestão da Impressão (MPS), a maioria dos fornecedores oferecem não só uma avaliação completa, mas também uma monitorização constante dos dispositivos, uma vez que o parque de impressão tenha sido otimizado e assegurado.

Trocar as palavras-passe pré-configuradas

As palavras-passe pré-configuradas ou por defeito são um ponto débil para os dispositivos de impressão. A boa notícia é que isto se pode resolver facilmente. Depois de instalado o equipamento, apenas terá de a alterar escolhendo uma que seja fiável e segura.

Atualização de firmware

É possível reduzir significativamente as potenciais vulnerabilidades de segurança dos equipamentos de impressão atualizando o firmware e configurando-o para que realize atualizações automáticas. No caso de dúvidas, o melhor é contactar o fabricante e pedir ajuda.

Proteger as impressões

Não só os equipamentos de impressão necessitam proteção, mas também os documentos que enviamos para imprimir. A encriptação do tráfego da rede, de ponta a ponta, assegura uma transferência segura dos trabalhos para o equipamento de impressão. E tendo em conta que a maioria das impressoras guarda temporariamente os trabalhos na sua memória, há que assegurar que os dados estão encriptados.

Monitorizar os equipamentos

Conhecer o estado atual do nosso parque de impressão oferece uma visão global de todo o ambiente de impressão. As empresas deveriam considerar o uso de ferramentas de software para monitorizar os equipamentos. Normalmente, estes podem gerar grande quantidade de dados que podem ser usados para identificar potenciais problemas de segurança e permitir uma resposta rápida aos ataques. Os utilizadores dos Serviços de Gestão de Impressão também podem obter regularmente, relatórios de conformidade, que deveriam incluir monitorização, e relatórios de possíveis falhas de dados.

Formar os colaboradores

Há muitas perdas de dados não intencionais e por isso é vital que as empresas formem os seus colaboradores sobre a importância de proteger a informação sensível e difundam informação sobre ameaças maliciosas. Muitas vezes, os fornecedores dos Serviços de Gestão da Impressão oferecem ajuda com estas necessidades de formação.

Conclusões

No passado, os sistemas de impressão podem ter sido esquecidos nos planos da segurança organizacional, mas as empresas já estão a dar conta da sua importância. No entanto, ainda há desafios significativos na implementação de medidas de segurança na impressão.

As empresas têm de definir claramente responsabilidades sobre a segurança da impressão para garantir que os dispositivos estão bem protegidos e podem resistir às ameaças. Assim, como a segurança do equipamento, as falhas de segurança dos dados são também de vital importância e a cooperação de todos os colaboradores é necessária para minimizar riscos.

Inclusivamente tendo uma definição clara das responsabilidades dentro das empresas, contar com os suficientes conhecimentos para manusear a segurança da impressão de forma eficiente é ainda um desafio importante. A tecnologia de impressão é cada vez mais complexa. As empresas deveriam tratar de confiar nos seus fornecedores para tomar decisões acertadas.

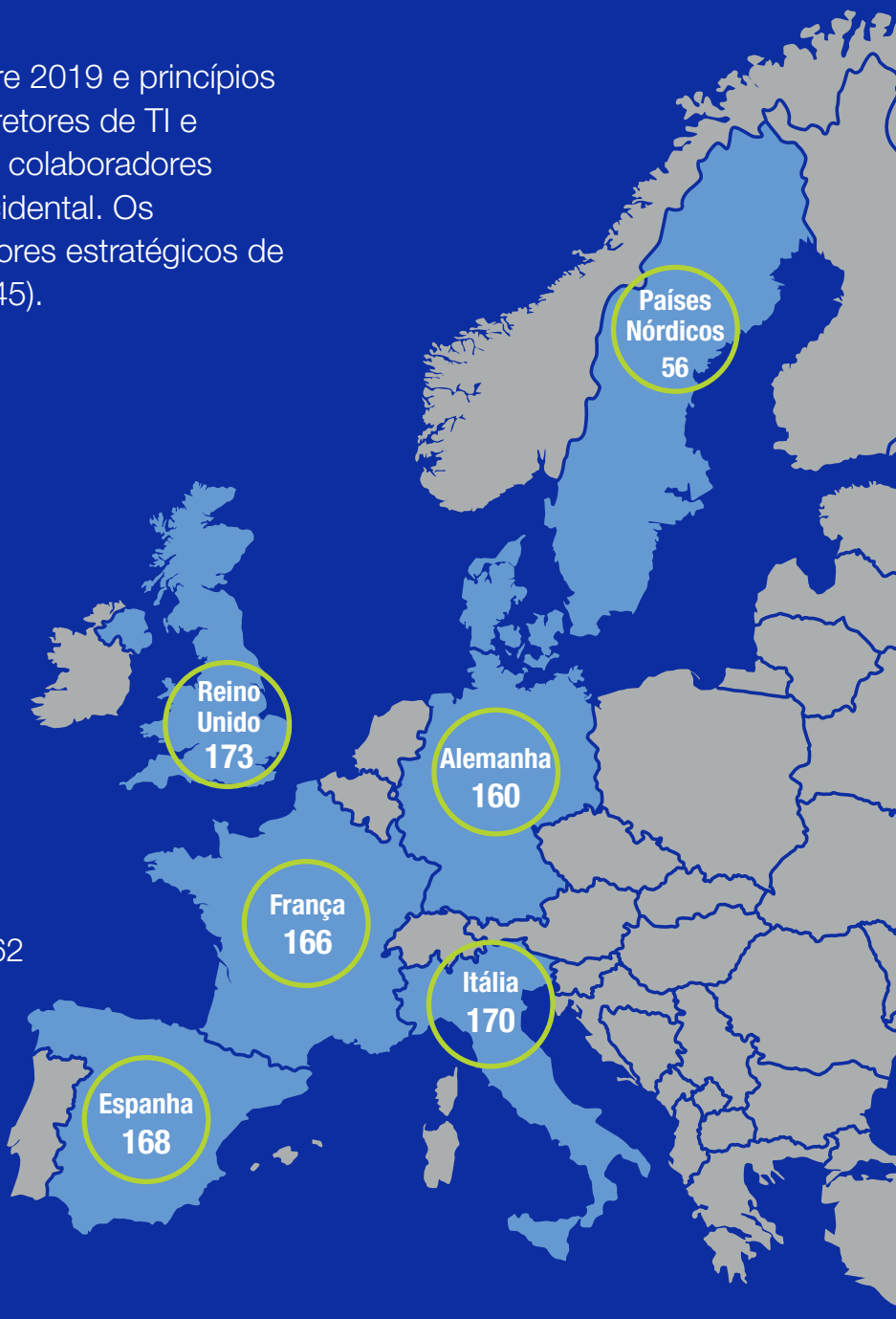
Um equipamento de impressão eficiente tem de ser mais que seguro.

Os restantes relatórios desta série de Transformação Digital oferecem mais informação sobre como implementar fluxos de trabalho digitais, maximizar a produtividade e assegurar que são sustentáveis.

A nossa metodologia

Este relatório baseia-se em 893 questionários online a responsáveis de empresas e de TI.

O trabalho de campo foi realizado entre 2019 e princípios de 2020, onde foram entrevistados diretores de TI e decisores de empresas com 10 a 499 colaboradores de diferentes mercados da Europa Ocidental. Os questionários dividiram-se entre decisores estratégicos de negócio (448) e responsáveis de TI (445).



Setores chave entrevistados:

- Saúde - 152
- Retalho - 117
- Logística - 113
- Hotelaria - 81
- Transporte e armazenamento - 62
- Serviços profissionais - 65
- Fabricantes - 54
- Serviços financeiros - 53
- Educação - 51
- Construção - 39

Também se realizaram entrevistas noutros setores incluindo energético, farmacêutico, agrícola, jurídico, imobiliário, desporto e entretenimento.

O relatório foi realizado pela empresa de estudos de mercado Savanta.

Obtenha a série completa

Outros relatórios da série Transformação Digital realizados pela Brother.

brother
at your side

brother.pt

Brother Ibéria, S.L.
Edifício Brother
Rua da Garagem, nº7
2790-078 Carnaxide
Tel: 808 223 000