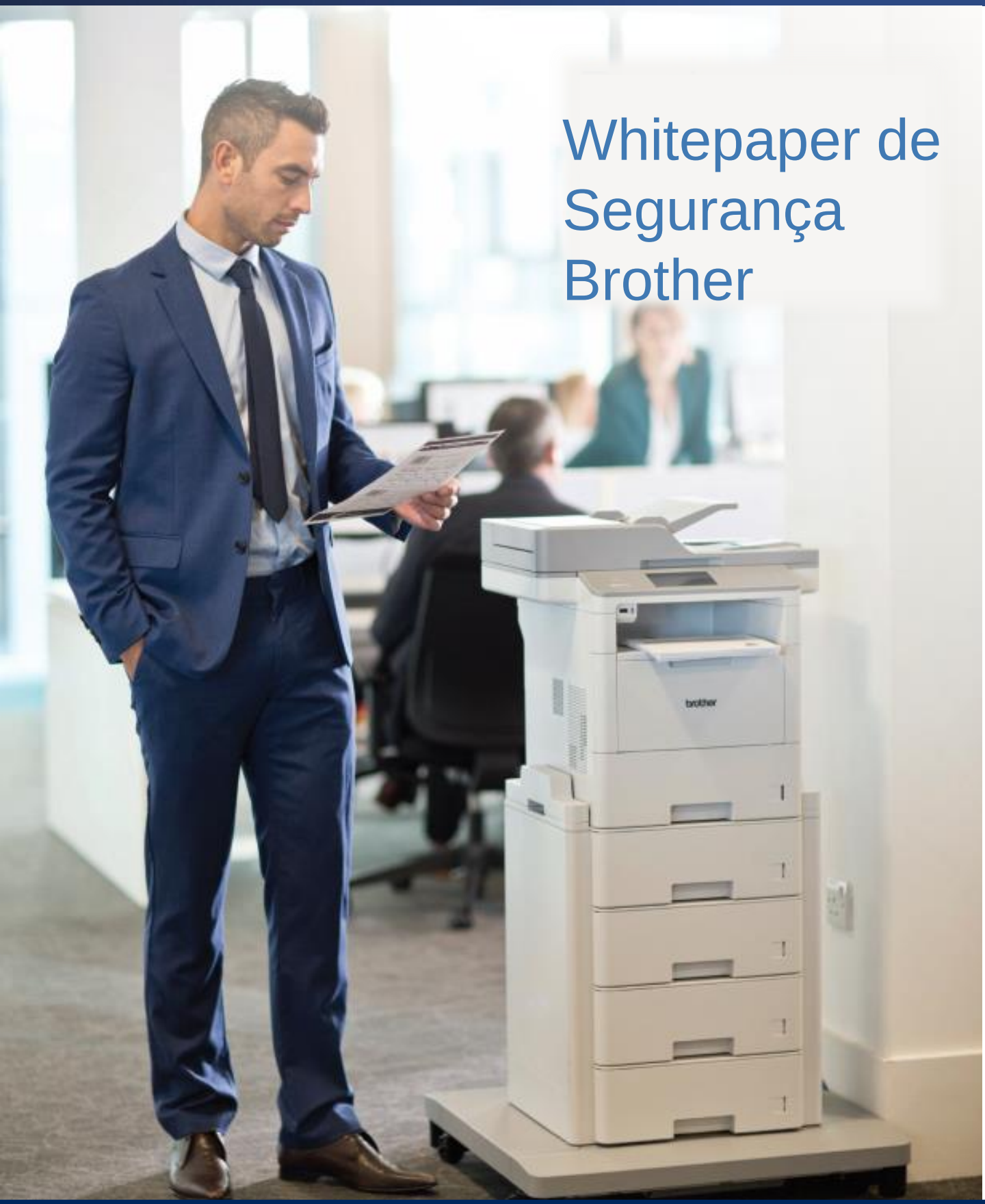


Whitepaper de Segurança Brother

AS AMEAÇAS OCULTAS EXPOSTAS PELA SUA IMPRESSORA

(E O QUE PODE FAZER CONTRA ISSO)

O parque instalado de impressoras e scanners nas empresas dispõe de uma versatilidade e potencialidade de crescimento. Mas todos estes avanços vêm acompanhados de maiores riscos para a segurança e são poucas as organizações que tomam suficientes medidas para se protegerem.

As medidas de segurança no trabalho constituem uma parte habitual da nossa vida quotidiana. Para proteger os ativos, as organizações utilizam elementos que vão desde os cartões ou códigos de identificação, até ao controlo de acesso físico, desde o uso do software de segurança da rede até à proteção de acesso à informação. Inclusivamente a ideia de ter uma conta de correio eletrónico sem password nos parece completamente imprudente.

A forma como os equipamentos informáticos, tais como impressoras e scanners, se conectam a redes teoricamente seguras também deve ser tida em conta para evitar debilidades na segurança das organizações.

Em 2015 a Brother realizou um estudo[1] sobre os desafios que enfrentam as empresas, no qual participaram mais de 2.500 pequenas e médias empresas.

75% destas considerou que a segurança da informação constituía um elemento muito importante para a sua organização, enquanto que 59% concordava que a segurança da informação afeta as decisões sobre a gestão de documentos e impressão.

Estas preocupações estão a ter cada vez mais relevância como resposta a um crescente número de problemas relacionados com a segurança em todos os setores de atividade. Um estudo da Quocirca[2] sobre uma amostra de 200 empresas que também foi levado a cabo em 2015 revelou que, pela primeira vez, a segurança está entre as maiores prioridades, com cerca de 75% de respostas que indicavam que era um fator importante ou muito importante. Em termos globais, 74% das organizações já pôs em marcha ou tem planificado implementar soluções de impressão segura.

Em que consistem exatamente estas ameaças?

Basicamente, há 4 formas nas quais os equipamentos de impressão ou scanners podem representar uma ameaça para a organização.

1. ATRAVÉS DA FUGA ACIDENTAL DE INFORMAÇÃO CONFIDENCIAL IMPRESSA
2. ATRAVÉS DA FUGA ACIDENTAL DE INFORMAÇÃO CONFIDENCIAL DIGITALIZADA
3. AO PERMITIR QUE EXISTAM INTRUSÕES NA REDE ATRAVÉS DE UM NÍVEL DE SEGURANÇA REDUZIDO
4. AO PERMITIR O ACESSO FÍSICO DE UTILIZADORES NÃO AUTORIZADOS A EQUIPAMENTOS NÃO VIGIADOS

Para ajudar as empresas a eliminar estas ameaças comuns para a segurança, a Brother elaborou um resumo dos riscos específicos que os administradores devem ter em conta, assim como o tipo de tecnologia que se desenvolveu especificamente e que se pode integrar com a segurança existente, com a finalidade de melhorar o nível de proteção.

1. ATRAVÉS DA FUGA ACIDENTAL DE INFORMAÇÃO CONFIDENCIAL IMPRESSA

Quais são os perigos?

Independentemente do nível de eficácia da política de segurança da sua empresa, se alguém pode aceder a uma impressora e recolher trabalhos que não são seus, esses dados estarão em perigo.

O posto de trabalho da maioria das pessoas não está exatamente à frente da impressora que utilizam, desta forma existe sempre risco de que os seus trabalhos não sejam imediatamente recolhidos e fiquem expostos a qualquer pessoa que se desloque ao equipamento ou até mesmo que passe por ele.

O que podem as empresas fazer relativamente a estes perigos?

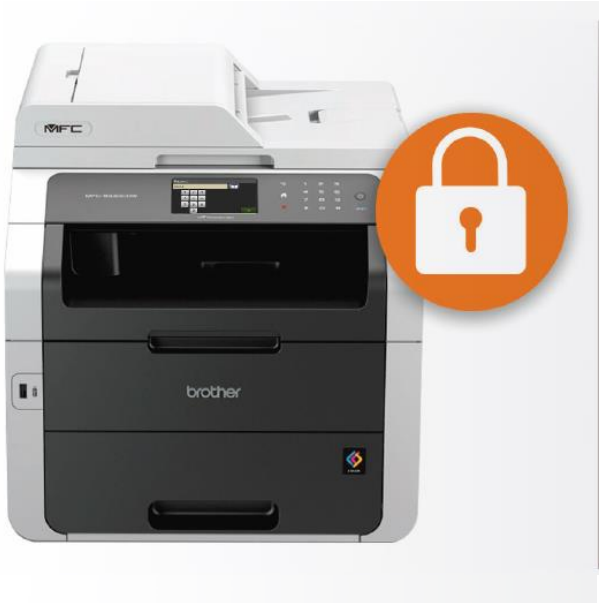
A melhor forma de combater eficazmente este risco é apenas efetuar a impressão quando o utilizador que deu ordem chegue à impressora e o modo ideal é fazê-lo através da introdução de um código ou um leitor de cartões de segurança. Em função do tamanho da empresa e dos seus requisitos, a Brother recomenda diferentes soluções. Uma delas é a **Impressão Segura**, uma funcionalidade desenhada principalmente para pessoas que imprimem documentos confidenciais de forma ocasional. A Impressão Segura permite aos utilizadores iniciar o processo de impressão quando estão fisicamente junto do equipamento, ou seja, se necessitar imprimir um trabalho confidencial, apenas tem que atribuir um código PIN à tarefa no controlador de impressão ao enviá-la para o equipamento. Mas se imprimem documentos confidenciais com maior frequência o melhor é utilizar a identificação por **Active Directory** que será mais efetiva. Esta funcionalidade restringe totalmente o acesso a qualquer função do equipamento, através do bloqueio a todas as pessoas não autorizadas. Para desbloquear o equipamento de impressão e recuperar o documento, os utilizadores devem previamente autenticar-se através do nome de utilizador e palavra-passe do Active Directory do Windows já criados. Neste caso e no da Impressão Segura, a tarefa fica armazenada na memória do equipamento até ser recolhida.

Para implementar a funcionalidade Active Directory, a empresa deve já utilizar o Active Directory da Microsoft. Não obstante, no caso das empresas que não o façam, existem soluções como a Impressão Segura com servidores de bases de dados de utilizadores, compatíveis com LDAP. Esta opção funciona da mesma forma que o Active Directory, mas comunica com o servidor através do protocolo LDAP habilitado.

Para aumentar o nível de segurança com as funções de Active Directory ou LDAP, os administradores podem especificar um limite de tempo durante o qual as tarefas de impressão não recolhidas são conservadas em memória nos equipamentos. Deste modo, os documentos confidenciais não permanecem esquecidos por tempo indeterminado na máquina.

No caso de ambientes onde as necessidades de impressão de informação confidencial variam em função dos utilizadores, será mais adequado uma **configuração baseada em rede**, uma solução que armazene os documentos num servidor central em vez de o fazer nos equipamentos. Isto permite recolher os documentos em qualquer equipamento de impressão do edifício que esteja conectado ao servidor mediante a utilização de um código a introduzir na impressora ou, quando for compatível, utilizando um cartão NFC. Além disso, os administradores podem ainda monitorizar com mais detalhe a utilização dos equipamentos por parte dos utilizadores.

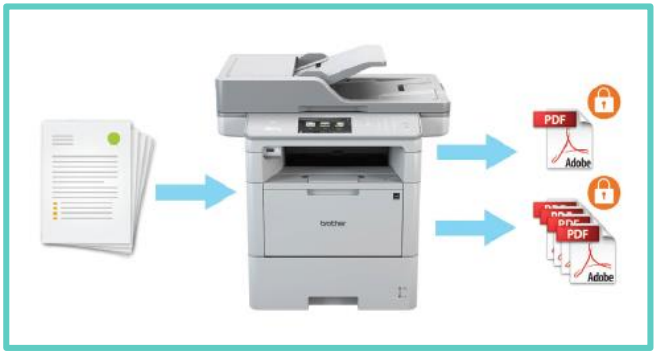
No entanto, mesmo aplicando todas estas medidas, continua a existir um ponto mais débil: com o software adequado, é possível intercetar os dados durante a sua transmissão para o equipamento. Para se proteger disto, a Brother recomenda a **encriptação de TLS (Transport Layer Security) e de SSL (Secure Socket Layer)**: a mesma tecnologia que se utiliza no comércio eletrónico para proteger os dados bancários e os cartões de crédito. Deste modo, ficheiros confidenciais podem ser encriptados com chaves até 256 bits durante a sua transmissão através da rede.



2. ATRAVÉS DA FUGA ACIDENTAL DE INFORMAÇÃO CONFIDENCIAL DIGITALIZADA

Quais são os perigos?

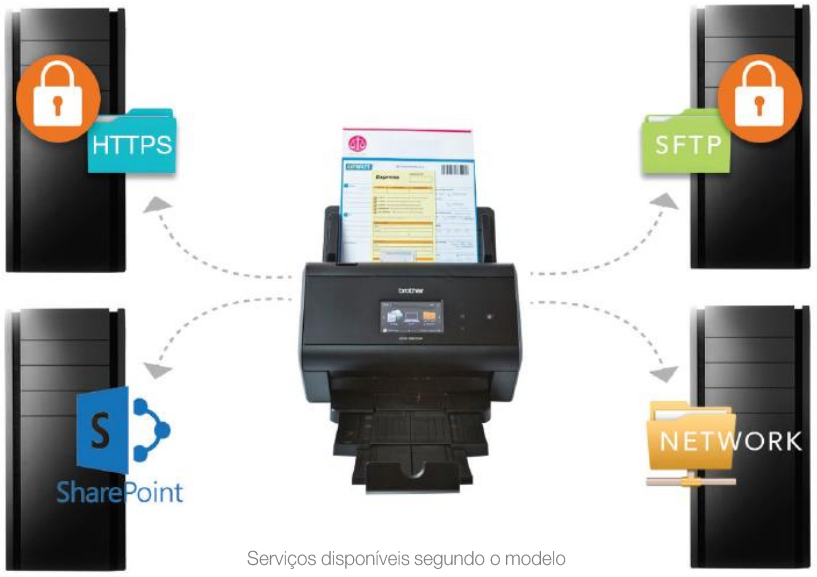
Mesmo que o seu equipamento de impressão ou digitalização seja seguro, existe outro risco de fuga de informação: através dos documentos digitalizados. Depois de digitalizar um documento confidencial, os utilizadores têm diversas opções para o arquivar ou partilhar. Partilhar documentos digitalizados por e-mail ou carregá-los na web são estratégias que comportam algum risco para as informações mais sensíveis, uma vez que os documentos podem cair nas mãos erradas muito rapidamente se for cometido um pequeno erro. E pior, não há limite relativamente à quantidade de cópias que se podem efetuar.



O que podem as empresas fazer relativamente a estes perigos?

A solução mais simples passa por converter o documento digitalizado num **PDF Seguro** protegido por um código, de forma a que ninguém o possa abrir sem a sua permissão.

Em alternativa, podem utilizar a função **digitalizar a SFTP (Secure File Transfer Protocol)**. Este protocolo seguro de transferência de ficheiros estabelece um fluxo de dados privado e seguro. Mediante o controlo de acesso aos servidores SFTP mais restrito, as empresas podem contribuir para manter toda a sua rede ainda mais segura através do fecho completo de uma porta de entrada e saída do seu sistema.



Serviços disponíveis segundo o modelo

3. AO PERMITIR QUE EXISTAM INTRUSÕES NA REDE ATRAVÉS DE UM NÍVEL DE SEGURANÇA REDUZIDO

Quais são os perigos?

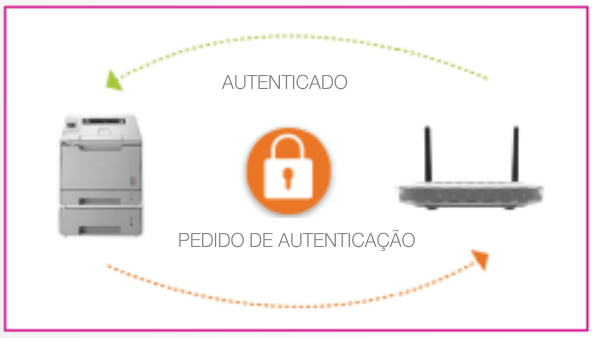
A necessidade de facultar certificados, nomes de utilizador e palavras-passe para conectar tablets e portáteis a uma rede segura é uma prática comum. Mas normalmente não se espera que seja necessário fazer o mesmo com todos os equipamentos de impressão ou digitalização, apesar de poder representar o mesmo nível de ameaça para a segurança.

O que podem as empresas fazer relativamente a estes perigos?

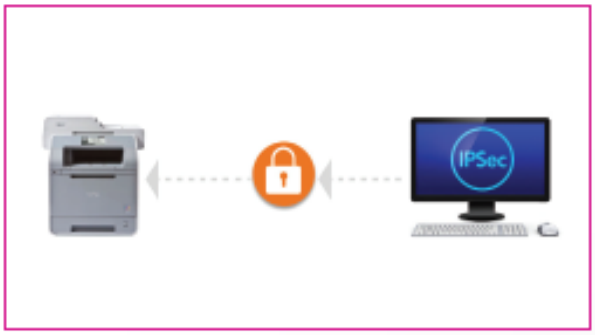
Ameaças externas

Como os seus dispositivos contam com diversos tipos de encriptação integrada, a Brother pode sugerir várias formas de melhorar a segurança e evitar possíveis fugas.

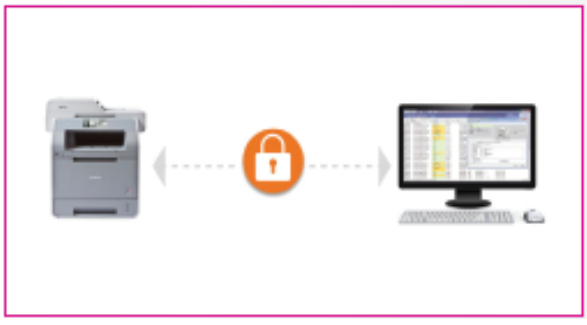
802.1x: é standard da IEEE para um acesso de rede autenticado a redes Ethernet por cabo e redes 802.11 sem fios. IEEE 802.1x melhora a segurança e a implementação ao proporcionar compatibilidade com identificação de utilizadores, autenticação, gestão de passwords dinâmicas e criação de contas de forma centralizada. É utilizado com os dispositivos conectados através de cabo ou que formem parte da infraestrutura sem fios da empresa.



IPsec: Internet Protocol security é um conjunto de protocolos cuja função é assegurar as comunicações sobre o Protocolo de Internet (IP) autenticando e/ou encriptando cada pacote IP num fluxo de dados. O IPsec também inclui protocolos para o estabelecimento de chaves de encriptação. Permite conectar vários dispositivos diretamente a ambientes seguros internos ou externos através de IPsec, o que permite poupar tempo e dinheiro. Como os equipamentos Brother têm IPsec integrado, não há necessidade de instalar software ou hardware de terceiros.



SNMPv3: é um protocolo da camada de aplicação que facilita a troca de informação de gestão entre dispositivos da rede. Este protocolo faz parte do conjunto de protocolos TCP/IP e permite aos administradores supervisionar o funcionamento da rede, procurar e resolver os seus problemas.



Os dispositivos Brother, que foram desenvolvidos para cumprir políticas de segurança de rede restritas, são capazes de interpretar todas as instruções que recebem nas versões 1, 2 e 3 (MD5 e SHA1) do SNMP encriptado, inclusivamente durante a configuração remota e a manutenção de rotina.

As organizações que utilizem a sua própria ferramenta de gestão do parque instalado para uma gestão centralizada, também devem implementar medidas de segurança para prevenir um acesso não autorizado.

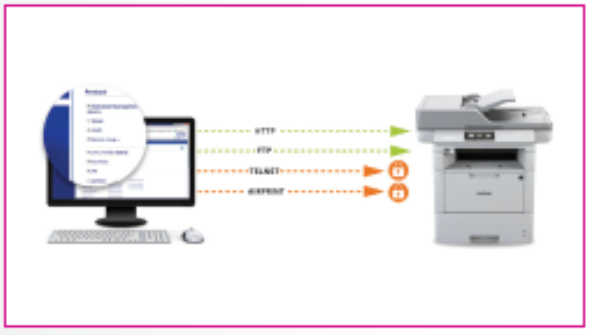
Ameaças internas

É certo que a encriptação oferece proteção contra as ameaças externas, mas o pessoal interno pode aceder remotamente a equipamentos conectados à rede e como tal a empresa pode tornar-se vulnerável. Para evitar qualquer problema derivado a isto, os equipamentos de impressão ou digitalização com **servidores web integrados, devem ter proteção por password**, que deixarão de estar disponíveis depois de um período de inatividade de cinco minutos.

Também é recomendável a função de **bloqueio de IP**, que impede o acesso ao dispositivo através da rede. Neste exemplo, a impressora apenas aceitará conexões de utilizadores dos seguintes IP: 10.45.12.1, 12.45.12.45, 10.45.12.46 e 10.45.12.47.

Se o que pretende é uma solução menos restritiva, o **Controlo de protocolos** permite aos administradores desabilitar protocolos que não sejam necessários, sem bloquear por completo o acesso a todos os elementos, como o FTP ou SMTP.

No exemplo em baixo, vê-se como o administrador do sistema desabilitou as seguintes funções: Telnet, AirPrint, Proxy e o servidor FTP:



4. AO PERMITIR O ACESSO FÍSICO DE UTILIZADORES NÃO AUTORIZADOS A EQUIPAMENTOS NÃO VIGIADOS

Quais são os perigos?

Apesar de contarem com todas estas funções de segurança, a menos que os equipamentos de impressão ou digitalização estejam protegidos fisicamente em salas seguras, as pessoas podem aproximar-se deles e tentar retirar informação dos mesmos. No caso de pequenas e médias empresas com pouca ou nenhuma infraestrutura informática, é particularmente importante ter algum tipo de segurança física.

No estudo realizado pela Brother em 2015, dois terços dos responsáveis pela tomada de decisão indicaram que a segurança afeta as decisões sobre a gestão de documentos e impressão e que, entre as questões que os preocupam, se encontra o modo como são conservados os documentos no equipamento de impressão.

O que podem as empresas fazer relativamente a estes perigos?

Para este tipo de organizações, recomendamos funções de segurança que evitam que as pessoas não autorizadas possam manipular os equipamentos.

Bloqueio de configuração: restringe o acesso à configuração do dispositivo através do painel de controlo. É ideal para organizações que não querem limitar a forma como as pessoas utilizam as funções, mas que queiram impedir os utilizadores não autorizados a modificar as configurações.

Bloqueio Seguro de Funções: vai um pouco mais além, uma vez que impede o acesso tanto à configuração do equipamento como a determinadas funções. Isto permite aos administradores decidir quem pode fazer o quê com cada máquina. Por exemplo, controlando que utilizadores podem enviar faxes e digitalizar documentos ou implementando limites mensais através de códigos ou cartões de acesso NFC únicos.

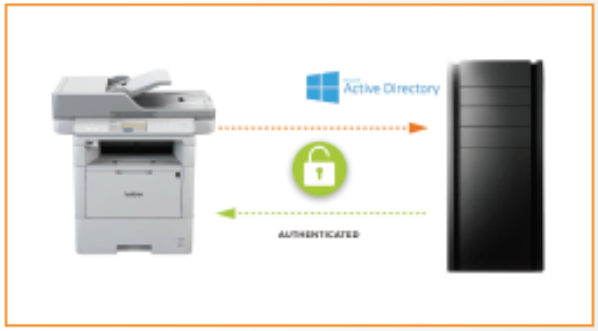
A imagem que mostramos de seguida corresponde à página de configuração do Bloqueio Seguro de Funções desde o servidor web integrado do dispositivo.

No chamado Modo Público, primeira linha da tabela, vimos que todas as funções estão bloqueadas para os utilizadores não autorizados. O Utilizador 1, não tem acesso restringido a nenhuma função.

Lista de usuarios / Funciones restringidas		Funciones										Límites de páginas (*)		
		Imprimir	Copia	Escanear	Fax		USB		Web Connect		Activado	Páginas máx.	Impresión a color
					Enviar	Recibir	Impresión directa*	Escanear a	Carga	Descarga			
	Modo público	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	0	☐
1	Usuario 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	0	☑
2	Usuario 2	☑	☑	☑	☐	☐	☑	☑	☑	☑	☑	100	☑

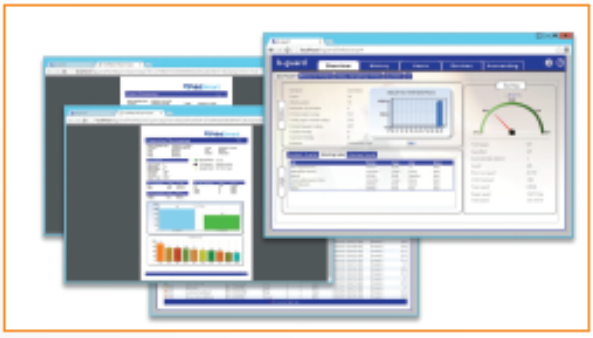
O Utilizador 2, tal como aparece na segunda linha, não pode enviar nem receber faxes e tem um limite de impressão de 100 páginas. Este limite pode ser ajustado e reiniciado por um administrador ou ser configurado para que se reinicie de forma periódica.

No caso de empresas nas quais vários utilizadores partilham equipamentos de impressão ou digitalização, ou onde é necessário colocá-los em locais públicos, pode ser difícil ter um controlo do uso abusivo sem dificultar o uso normal. No entanto, com as opções de Active Directory ou de autenticação LDAP, o pessoal pode utilizar de forma simples as suas credenciais de início de sessão já existentes para ter acesso aos equipamentos em utilização.



Recomendações

Não há dúvida de que muitas empresas de todos os setores devem levar a sério as ameaças para a segurança de dados e redes que possuem equipamentos de impressão e scanners, mas não existe uma solução única. Os administradores de sistemas têm que selecionar as soluções adequadas de acordo com as características particulares dos seus riscos, infraestruturas e segurança existentes.



Resumindo, uma empresa deve:

1. Garantir a segurança dos seus equipamentos;
2. Proteger os dados durante e após a impressão;
3. Proteger a sua rede de intrusos.

Uma vez assegurados estes pontos, poderá confiar que os seus sistemas de impressão e digitalização contarão com uma proteção adequada face às ameaças para a segurança, no futuro próximo.

[1] Fonte: estudo sobre pequenas e médias empresas realizado por B2B International a 2502 empresas do Reino Unido, França, Alemanha e Estados Unidos.

[2] Fonte: Quocirca Managed Print Services Landscape (Panorama dos serviços de gestão de impressão de Quocirca), 2015. Inquérito a 200 empresas, com 1000 ou mais colaboradores, do Reino Unido, França, Alemanha e Estados Unidos.