Guia de referência de segurança da Lexmark

Quando o assunto é segurança, sua organização precisa ter certeza de que pode gerenciar os dispositivos de rede de forma segura, defendê-los contra hackers e proteger fisicamente os dados armazenados. Por esse motivo, na Lexmark, desenvolvemos impressoras e multifuncionais compatíveis com soluções para atender a essas necessidades.

Gama completa de segurança

A segurança é integrada a cada produto da Lexmark, com recursos de segurança padrão apropriados para cada uso pretendido do produto e opções disponíveis para atender a exigências especiais. Nossa abordagem completa da segurança de produtos da Lexmark abrange uma gama completa de recursos de segurança.

- **Os recursos de acesso seguro** restringem quem pode usar seus dispositivos e o que eles podem fazer.
- **Os recursos de segurança de rede** protegem os dispositivos contra acesso não autorizado a interfaces de rede.
- **Os recursos de segurança de documentos** mantêm seus documentos — sejam físicos ou virtuais — longe da vista ou das mãos erradas.
- **O gerenciamento remoto seguro** oferece uma ampla variedade de ferramentas e recursos de dispositivos para gerenciar de maneira eficaz uma frota de multifuncionais e impressoras a laser em rede.
- **As soluções de segurança** aumentam a segurança dos dispositivos da Lexmark e de seu ambiente ao cumprir objetivos específicos, como liberação de impressão*, certificado de segurança automática e Monitor de Conteúdo Seguro.
- **A segurança de disco rígido** protege as multifuncionais e impressoras da Lexmark que contêm discos rígidos internos com um escudo virtual para conservar os segredos de sua organização.

*Opcional

Recursos de acesso seguro

Quem é você? A maioria das violações de segurança ocorre quando um usuário finge ser quem não é. Os dispositivos da Lexmark foram desenvolvidos para fornecer acesso livre aos usuários certos e, ao mesmo tempo, impedir a entrada dos impostores.

Flexibilidade de autenticação e autorização: Os dispositivos da Lexmark podem ser configurados para validar credenciais de usuário e restringir funções de dispositivos usando o Active Directory e outras plataformas de servidor de diretório, incluindo contas internas, NTLM, Kerberos 5, LDAP, LDAP+GSSAPI, senha e PIN.

Segurança de usuário e grupo: Conceda a usuários individuais e conjuntos de usuários o direito de acessar funções de dispositivos específicas e, ao mesmo tempo, restrinja outros usuários ou grupos.

Controles de acesso: Controle o acesso local e remoto a menus, funções e fluxos de trabalho específicos em cada dispositivo. Desative totalmente funções como cópia, impressão, fax, digitalização para e-mail, FTP, trabalhos retidos e catálogo de endereços. Mais de 50 controles de acesso estão disponíveis, fornecendo maior flexibilidade para seu ambiente exclusivo.

Modelos de segurança: Os administradores do dispositivo podem restringir facilmente o acesso ao dispositivo combinando privilégios de grupo, controles de acesso e métodos de autenticação em modelos de segurança que são exibidos no menu suspenso Controle de acesso. A abrangência de um modelo de segurança é grande, fornecendo controle de algumas das configurações de segurança mais importantes no dispositivo da Lexmark.

Portas USB protegidas: As impressoras e multifuncionais a laser da Lexmark incluem suporte para dispositivos USB, que podem causar problemas em ambientes onde a segurança é fundamental. Desenvolvidas com segurança em mente, as portas de host USB têm vários mecanismos para impedir seu uso de maneira prejudicial.

Inserção automática do endereço de e-mail do remetente: Quando um usuário se autenticar para digitalizar um documento e enviá-lo por e-mail, o endereço de e-mail do remetente será automaticamente pesquisado e inserido no campo"De". Assim, o destinatário poderá ver claramente se o e-mail foi gerado por aquela pessoa e não anonimamente ou pela multifuncional.

Restrições de login: Você pode impedir o uso não autorizado de um dispositivo restringindo o número de logins consecutivos com falha—e rastrear esses eventos com uma auditoria integrada. Quando esse limite é excedido, o dispositivo é bloqueado por um período predeterminado especificado pelo administrador.

Bloqueio do painel do operador: O recurso Bloqueio do painel do operador permite que uma multifuncional seja bloqueada, impedindo que o painel do operador seja usado para executar operações ou configurações do usuário. É possível desbloquear o dispositivo fornecendo as credenciais de um usuário autorizado. Assim, a operação normal do dispositivo será restabelecida.

Retenção de fax recebido: Os dispositivos da Lexmark podem ser configurados para reter em vez de imprimir os faxes recebidos em períodos programados. Os faxes são retidos com segurança no disco rígido até que as credenciais apropriadas sejam fornecidas no dispositivo da Lexmark. As credenciais incluem, por exemplo, PIN, senha, além de ID de rede e senha do usuário.

Segurança de rede

A TI moderna é construída em torno da rede, mas a mesma conectividade que torna dispositivos em rede acessíveis para usuários autorizados pode colocar a integridade da rede e informações valiosas em risco sem as tecnologias e as garantias integradas aos dispositivos da Lexmark.

Filtragem de conexão TCP: Impressoras e multifuncionais podem ser configuradas para permitir conexões TCP/IP apenas de uma lista específica de endereços TCP/IP. Isso impede todas as conexões TCP de outros endereços, protegendo o dispositivo contra impressões e configurações não autorizadas.

Filtragem de portas: As portas de rede pelas quais as impressoras e multifuncionais ouvem ou transmitem o tráfego de rede são configuráveis, proporcionando alto nível de controle da atividade de rede do dispositivo. Com a filtragem do tráfego em portas de rede específicas, protocolos como telnet, FTP, SNMP, HTTP e muitos outros podem ser explicitamente recusados.

802.1x: Com a autenticação da porta 802.1x, as impressoras e multifuncionais podem ingressar em redes com e sem fio solicitando a autenticação dos dispositivos antes de acessar a rede. Essa autenticação pode ser usada com o recurso Wi-Fi Protected Access de um servidor de impressão sem fio opcional para oferecer suporte à segurança WPA empresarial.

IPsec: A opção de protocolo IPsec, quando ativada, protege todo o tráfego de rede de entrada e saída dos dispositivos da Lexmark com criptografia e autenticação. Isso protege os dados de impressão e o conteúdo dos trabalhos digitalizados para qualquer destino, incluindo os servidores que executam o Lexmark Document Distributor, e-mail e armazenamento de rede.

NTP seguro: Os dispositivos da Lexmark oferecem suporte ao SNTP (Secure Network Time Protocol) para sincronizar os relógios de vários dispositivos da rede. Para satisfazer o requisito principal de uma implementação SNTP, os dispositivos da Lexmark têm um campo de autenticador e autenticação na nossa configuração SNTP.

Separação de fax/rede: A Lexmark oferece diversos dispositivos multifuncionais que possuem conectividade de rede e recurso de modem de fax. E para impedir qualquer interação direta entre o modem e o adaptador de rede, o hardware e o firmware dos dispositivos da Lexmark mantêm esses mecanismos separados.

LDAP seguro: Todo o tráfego LDAP de entrada e saída de dispositivos da Lexmark pode ser protegido com TLS/SSL. As informações de LDAP, como credenciais, nomes, endereços de e-mail e números de fax trocados por uma conexão TLS/SSL, são criptografadas para preservar a confidencialidade e a privacidade dos dados.

Segurança dos documentos

Antigamente, as pessoas clicavam em "imprimir" em seus desktops, e as impressoras de rede imprimiam páginas em série que se acumulavam, deixando segredos expostos para qualquer um ler. Sabendo que você precisa imprimir muitos documentos e, ainda assim, proteger as informações que eles contêm, a Lexmark oferece uma variedade de recursos e produtos opcionais. Eles asseguram que somente pessoas autorizadas vejam saídas privadas, ao mesmo tempo que economizam papel e bens de consumo, proporcionando aos usuários móveis novas opções de impressão. Dessa forma, a Lexmark fortalece a segurança dos documentos.

Impressão confidencial: Uma parte-padrão do Driver de Impressão Universal da Lexmark, a Impressão confidencial retém seu trabalho em uma impressora ou multifuncional da Lexmark específica até que você o libere com um PIN. Isso evita que curiosos vejam documentos na bandeja de saída. Os trabalhos retidos podem ser configurados para expirar após determinado período (que varia de uma hora a uma semana). Além disso, é possível limitar o número de vezes que um PIN é digitado incorretamente antes que os trabalhos correspondentes sejam excluídos. Como em todas as formas de liberação de impressão, você só paga pelas páginas impressas de fato—e não pelas páginas que alguém imprimiu, mas nunca recolheu.

Aplicativo de Trabalhos seguros retidos: Impeça a exposição acidental de informações comerciais importantes ou confidenciais retendo os trabalhos em um dispositivo específico até que um usuário autorizado vá até ele e libere o trabalho para impressão. Essa é a premissa básica do aplicativo eSF Trabalhos seguros retidos* para dispositivos inteligentes, que permite aos usuários enviar e armazenar trabalhos na impressora ou multifuncional e liberá-los quando quiser usando um PIN de quatro dígitos ou um cartão de identificação.

Liberação de impressão segura: O Gerenciamento de Impressão da Lexmark* permite que os usuários enviem trabalhos de qualquer lugar e os recolham em qualquer dispositivo configurado para liberação de impressão na rede. Você terá maior flexibilidade de impressão, evitará que os documentos se acumulem nas impressoras, protegerá a confidencialidade dos documentos que, de outra forma, poderiam ficar expostos, e economizará em custos de impressão. E todo o processo de liberação é protegido por credenciais inseridas no dispositivo, na forma de identificação de usuário de rede ou de um crachá de identificação.

Opções como essas ajudam a Lexmark a garantir a segurança do documento em qualquer trabalho de impressão e qualquer fluxo de trabalho.

*Opcional

Gerenciamento remoto seguro

Para gerenciar com praticidade uma frota de dispositivos de criação de imagem e impressão em rede, o gerenciamento remoto seguro é obrigatório. O dispositivo deve permitir que pessoas autorizadas o configurem e, ao mesmo tempo, rejeitar pessoas não autorizadas. O processo de gerenciamento do dispositivo também deve ser protegido, de forma que o tráfego de rede associado ao gerenciamento remoto não possa ser capturado, roubado ou utilizado indevidamente.

Os dispositivos da Lexmark incluem diversos recursos para tornar o gerenciamento de dispositivo remoto mais fácil e mais seguro. Esses recursos podem ser configurados na página da Web incorporada do dispositivo.

Acesso a dispositivos e configurações: O que torna as impressoras e multifuncionais (MFPs) da Lexmark inteligentes é sua capacidade de executar e configurar aplicativos que automatizam tarefas manuais, melhoram a segurança e orientam os usuários nos processos de negócios com facilidade. Mas como qualquer dispositivo programável com opções de configuração abrangentes, eles devem ser protegidos cuidadosamente como qualquer PC ou servidor da rede. Os dispositivos da Lexmark incluem uma variedade de controles de acesso de função, mecanismos de autenticação e autorização, além de uma senha de backup opcional para impedir que usuários não autorizados alterem as configurações do dispositivo, incluindo configurações de segurança.

Registro de auditoria em log: Rastreie eventos relacionados a segurança para reduzir a exposição, rastreie e identifique proativamente riscos em potencial e integre ao seu sistema de detecção de intrusão para rastreamento proativo em tempo real.

Firmware criptografado e digitalmente assinado: As impressoras e multifuncionais da Lexmark inspecionam automaticamente as atualizações de firmware baixadas para obter as assinaturas digitais apropriadas da Lexmark. O firmware que não é corretamente compactado e assinado pela Lexmark é rejeitado.

A tecnologia de inicialização segura valida que o firmware instalado na impressora é original da Lexmark. Quando um firmware não original é detectado, os usuários recebem uma notificação.

A verificação contínua garante que o firmware não foi violado durante a operação.

Gerenciamento de certificados: As impressoras e multifuncionais usam certificados para autenticações HTTPS, SSL, IPsec e 802.1x. O recurso Gerenciamento de certificados permite que os dispositivos se integrem a um ambiente de PKI. Desse modo, os certificados podem ser assinados e os dispositivos podem confiar nas autoridades de certificado no ambiente de PKI.

HTTPS: As impressoras e multifuncionais da Lexmark usam o protocolo de comunicação HTTPS. Isso permite que o tráfego da Web seja criptografado para que você possa realizar o gerenciamento remoto com segurança pela página da Web do dispositivo.

SNMPv3: A versão 3 do protocolo de gerenciamento de rede padrão SNMP inclui amplos recursos de segurança. As impressoras e multifuncionais da Lexmark são compatíveis com SNMPv3, incluindo os componentes de autenticação e criptografia de dados, para permitir o gerenciamento remoto seguro dos dispositivos. SNMPv1 e SNMPv2 também são aceitos e podem ser configurados ou desativados de forma independente.

Redefinição de senha segura: Caso uma senha administrativa seja perdida ou esquecida, ou se o dispositivo perder a conexão com a rede, o recurso de redefinição de senha segura redefinirá a configuração de controle de acesso no menu Segurança do dispositivo para permitir acesso.

Soluções de segurança

Sua impressora a laser ou multifuncional inteligente da Lexmark pode executar aplicativos relacionados a segurança para atender a necessidades especiais, como liberação de impressão*, registro de certificado de segurança automático e autenticação por SmartCard. Outra solução pode rastrear e fazer auditoria centralmente de todos os documentos impressos, copiados, digitalizados ou enviados por fax na rede.

Liberação de impressão segura: O Gerenciamento de Impressão da Lexmark* permite que os usuários enviem trabalhos de qualquer lugar e os recolham em qualquer dispositivo configurado para liberação de impressão na rede. Você terá maior flexibilidade de impressão, evitará que os documentos se acumulem nas impressoras, protegerá a confidencialidade dos documentos que, de outra forma, poderiam ficar expostos, e economizará em custos de impressão. E todo o processo de liberação é protegido por credenciais inseridas no dispositivo, na forma de identificação de usuário de rede ou de um crachá de identificação.

Registro de certificado automático (ACE): A criação de um certificado de dispositivo assinado por uma Autoridade de certificações (CA, Certificate Authority) para permitir que as conexões de SSL, IPsec e 802.1x sejam estabelecidas nos dispositivos de rede costuma ser um processo demorado. O ACE simplifica o processo para dispositivos habilitados para soluções da Plataforma A em um ambiente do Active Directory, exigindo a entrada de apenas um número limitado de parâmetros de controle de domínio e identidade de usuário.

Suporte a autenticação de cartão sem contato: As soluções de autenticação de crachá incluem soluções de cartão sem contato (aplicativos) para autenticação de crachá básica. Essa opção está disponível quando a identidade do usuário está vinculada a crachás de identificação de segurança do escritório. As soluções podem verificar o crachá de identificação e recuperar as informações do usuário, de forma que o dispositivo da Lexmark possa acessar trabalhos de impressão retidos, identificar a origem dos documentos digitalizados ou identificar um usuário por outros motivos.

Autenticação de cartão SIPR e CAC/PIV: As soluções de autenticação CAC (Common Access Card, Cartão de acesso comum) e PIV (Personal Identity Verification, Verificação de identidade pessoal)* proporcionam processos de fluxo de trabalho seguros para fornecer maior controle da segurança de multifuncionais da Lexmark em rede nas operações do governo federal. As funções de captura de informações digitais exigem uma autenticação de usuário forte para impedir o acesso não autorizado e proteger dados cruciais. A mesma solução também oferece suporte a cartões de token SIPR (Secret Internet Protocol Router, Roteador do protocolo de internet secreto) usando um aplicativo de interface de cartão diferente para fornecer acesso à rede correspondente.

Monitor de Conteúdo Seguro: Reduza os riscos e as responsabilidades associados a violações de segurança de documentos físicos. O Monitor de Conteúdo Seguro* pode simultaneamente monitorar e fazer auditoria das informações de milhões de documentos provenientes de todas as impressoras e multifuncionais, sejam eles impressos ou digitalizados, para melhorar a forma como a empresa detecta, investiga e detém infrações.

Segurança do disco rígido

Algumas impressoras e multifuncionais da Lexmark incluem discos rígidos internos para armazenar imagens de documentos impressos, digitalizados, enviados por fax ou copiados. O disco rígido interno também armazena dados que ampliam os recursos e as funcionalidades dos dispositivos. Esses dispositivos contêm uma ampla gama de recursos projetados cuidadosamente para melhorar a segurança dos dados armazenados no disco rígido e ajudar a impedir que usuários mal-intencionados tenham acesso a informações confidenciais.

Criptografia de disco rígido: O disco rígido de impressoras e multifuncionais pode ser configurado para usar criptografia. Uma chave AES, de até 256 bits, é gerada internamente pela impressora ou multifuncional e usada para criptografar todos os dados do disco rígido. A chave é armazenada de forma não contígua no dispositivo, deixando o conteúdo do disco rígido acessível somente na impressora ou multifuncional original. Os dados de um disco rígido roubado não seriam acessados mesmo se o disco rígido fosse instalado em uma impressora ou multifuncional do mesmo modelo.

Limpeza de arquivos de disco rígido: Os dados gravados nos discos rígidos da impressora ou multifuncional para uso temporário durante a impressão, a digitalização, o envio de fax ou a cópia podem ser apagados quando o trabalho é concluído ou após a impressão de um trabalho retido para um usuário. Para garantir que as informações nunca possam ser recuperadas, os discos rígidos da impressoras e multifuncionais da Lexmark removem a referência do arquivo no diretório do disco e apagam o arquivo no disco, impedindo a leitura de qualquer dado residual. Dependendo do dispositivo, a limpeza do disco rígido pode ser configurada para o modo manual, automático ou programado. Uma limpeza de várias camadas também é oferecida, de acordo com os padrões NIST/DOD.

Limpeza de disco rígido completa: Antes que uma impressora ou multifuncional seja desativada, reciclada ou removida de um ambiente seguro, um usuário autorizado por apagar o disco rígido completamente. Isso inclui a exclusão de formulários, fontes, macros e trabalhos retidos não impressos que a limpeza de arquivos de disco rígido de rotina (acima) pode deixar para trás. As opções de limpeza de camada única ou de várias camadas são oferecidas, garantindo que nenhum dado legível permaneça no disco.

Limpeza de memória não volátil: A limpeza de memória não volátil é uma ferramenta para apagar todo o conteúdo armazenado nas várias formas de memória flash contidas no dispositivo. Esse recurso apaga todas as configurações, soluções, trabalhos e faxes no dispositivo. Ele foi desenvolvido para ser usado quando o dispositivo da Lexmark for desativado, reciclado ou removido de um ambiente seguro.

Limpeza fora de serviço: Simplifique o processo de limpeza da unidade de disco de um dispositivo e dos dados da memória não volátil ao retirar uma unidade de serviço ou removê-la de um local seguro. Usuários autorizados podem fazê-lo em uma única etapa, com o comando de limpeza "fora de serviço", disponível no menu Configuração do próprio dispositivo, ou na página da Web do dispositivo.

Suporte a bloqueio físico: As impressoras e multifuncionais da Lexmark são compatíveis com bloqueios estilo Kensington, o que permite a proteção física dos dispositivos. Bloquear uma impressora ou multifuncional também bloqueia o gabinete de metal que armazena o disco rígido e outros componentes opcionais, ajudando a evitar falsificações ou roubo.

Padrões e certificações

Qualquer fabricante pode dizer que seus produtos são seguros. A Lexmark busca e obtém certificações para cumprir os padrões abrangentes do setor e do governo.

Common Criteria (Certificação NIAP/CCEVS, ISO 15408): O Common Criteria fornece uma estrutura para validar a funcionalidade de segurança de um sistema de computador. Essa validação de terceiros garante aos clientes que os recursos de segurança protegem o dispositivo conforme alegado pelo fabricante.

FIPS: O NIST (National Institute of Standards and Technology, Instituto nacional de padrões e tecnologia) fundamenta os requisitos e os padrões para módulos criptográficos no FIPS (Federal Information Processing Standards, Padrão de processamento de informações federal). A Lexmark concluiu o CAVP (Cryptographic Algorithm Validation Program, Programa de validação de algoritmo criptográfico) do FIPS 140-2 para produtos da Lexmark, uma validação independente que comprova a implementação correta dos algoritmos criptográficos usados em nossos dispositivos.

Saiba mais

Para obter mais informações sobre recursos de segurança, produtos e serviços da Lexmark, entre em contato com o representante da Lexmark ou fale conosco no número 888-403-2803.