DEVELOP

Dynamic balance

www.develop.eu

Segurança
em que pode confiar!

As normas de segurança da Develop

segurança de dados
de segurança
segurança

Normas de segurança líder da indústria

Nas empresas de hoje, a informação empresarial tem de atravessar muitas estradas de dados diferentes. Essas várias estradas oferecem uma série de oportunidades para ataques digitais por hackers ou vírus. É bom ter um software de antivirus, administradores de rede e outras ferramentas que ajudam a proteger o seu ambiente! Mas que tal o seu sistema digital de escritório? Tem protegido o seu sistema multifuncional tão bem como o seu PC?

Quase todos os processos e fluxos de trabalho começam, acabam ou estão de alguma forma relacionados com o seu equipamento multifuncional de escritório. Muita informação empresarial passa pelo seu sistema multifuncional. É por isso que o sistema multifuncional de escritório como elemento principal dos seus processos e fluxos de trabalho tem de suportar as ameaças contínuas contra a segurança.

A vasta gama de caraterísticas e opções de segurança da Develop representam uma fonte poderosa na qual podem ser baseadas as soluções profissionais: soluções para tanto detetar e prevenir violações de segurança, e evitar danos financeiros e/ou de reputação a nível corporativo bem como individual. A Develop foi pioneira nesta área e continua a ser o líder da indústria. Os sistemas da Develop são certificados, quase sem exeção, de acordo com a norma Common Criteria/ISO 15408 EAL3. Esses são as únicas normas internacionalmente reconhecidas de testes de segurança de TI para os produtos digitais de escritório. As impressoras, copiadoras e softwares compatíveis com a certificação ISO 15408 passaram todas por uma avaliação de segurança rigorosa e são capazes de satisfazer e oferecer os níveis de segurança que uma empresa prudente deveria procurar e ligitimamente esperar.

Os dados ficam onde pertencem – nas mãos certas!

Os sistemas ineo oferecem uma ampla variedade de funções e caraterísticas. Todas essas caraterísticas representam uma grande quantidade de potenciais falhas de segurança. Por esse motivo estão incluídos muitos mecanismos de segurança no sistema, oferecendo controlo de acesso seguro, segurança de documentos e de dados e segurança de rede. Com os sistemas ineo os dados ficam onde pertencem.

Controlo de acesso/Segurança de acesso

Apesar do tema de segurança estar no topo de agenda em ambos os domínios públicos e empresariais, os sistemas multifuncionais são muitas vezes ignorados como sendo qualquer tipo de risco de segurança. Isto é especialmente arriscado para aqueles sistemas e impressoras localizadas em zonas públicas, onde os funcionários, fornecedores e até visitantes podem ter acesso. Pelo facto que as caraterísticas avançadas dos atuais sistemas deliberadamente facilitam que a informação disponível no sistema seja copiada e distribuída dentro e além das fronteiras corporativas atuais e virtuais, o primeiro passo lógico é prevenir que pessoas sem autorização sejam capazes de trabalhar com o sistema multifuncional. As medidas preventivas têm de controlar o acesso aos sistemas multifuncionais.

Por esse motivo a Develop oferece várias caraterísticas e soluções de segurança que permitem o controlo de acesso e de segurança.

Segurança documental/ Segurança de dados

Pelo facto que os sistemas multifuncionais e impressoras estejam muitas vezes localizadas em zonas públicas onde podem ser acedidas com facilidade, a informação ou documentos confidenciais armazenados no disco rígido ou as impressões no tabuleiro de saída podem cair nas mãos erradas. Por este motivo será importante implementar políticas de segurança que garantem que os documentos e a informação não saiam da sua empresa. Para garantir a segurança de documentos e de dados a Develop oferece uma enorme variedade de caraterísticas de segurança feitas à medida!

Segurança de rede

O atual ambiente empresarial é caraterizado por sistemas conetados, recolha automática de dados e transmissão para sistemas de downstream para posterior tratamento de dados. Assim como a digitalização para uma pasta no PC ou para E-Mail. Os equipamentos de escritório da Develop são projetados para trabalhar em ambientes de rede que permitem fluxos de trabalho rápidos de processamento com a possibilidade de digitalizar informação para destinos de rede ou receber trabalhos de impressão a partir de vários equipamentos e destinos. Existe uma grande quantidade de conexões de e para o sistema multifuncional que precisam de ser protegidas. Caso contrário representam um potencial risco.

Por isso a Develop garante que todos os equipamentos estejam em conformidade com as normas de segurança mais rigorosas que são alcançadas por várias caraterísticas para fechar potenciais falhas de segurança utilizando uma ligação de rede.

Com a sua vasta gama de caraterísticas de segurança, a Develop fornece soluções profissionais para a deteção e prevenção de falhas de segurança.

Controlo & segurança de acesso – o caminho seguro para o multifuncional DEVELOP

As caraterísticas disponíveis nos sistemas multifuncionais tornam a sua operação muito fácil. O primeiro passo lógico é prevenir que pessoas sem autorização possam utilizar o sistema. Isto é o motivo da necessidade de autenticação incluindo a definição dos utilizadores, grupos de utilizadores, limites de acesso e direitos de utilização. Assim alguns utilizadores são autorizados para utilizar funções específicas, enquanto outros não.

Métodos de autenticação de utilizador

A DEVELOP oferece vários métodos de controlo de acesso que permitem o acesso ao multifuncional através da autenticação. Assim apenas pessoas autorizadas podem ter acesso e utilizar as funcionalidades do sistema.

› Autenticação biométrica por veias de dedo

A autenticação biométrica por veias de dedo representa a tecnologia de ponta ao trabalhar com imagens de padrões das veias de dedo que são capturadas pela digitalização do dedo. Ao utilizar uma caraterística humana pessoal para a identificação, essa medição biométrica é virtualmente impossível de falsificar. Este método de autenticação é muito mais seguro que os sistemas de impressão digital. E é rápido e simples, uma vez que não há necessidade de recordar palavras passe ou levar um cartão.

› Cartão IC de aproximação

A autenticação por cartão IC de aproximação também está disponível para a maioria dos sistemas ineo. Este método também foi projetado para a conveniência e rapidez – é simplesmente uma questão de passar o cartão IC sobre ou perto do leitor.

› Palavra passe ou código de utilizador

A forma mais simples de autenticação de utilizador é restringir o acesso por uma palavra passe pessoal ou código de utilizador que tem de ser introduzido no painel. Esta autenticação interna no sistema suporta até 1,000 contas de utilizador. As palavras passe são alfanuméricas com até 64 caratéres, podem ser criadas para administradores e utilizadores e são geridas pelo administrador.

Mais caraterísticas de autenticação

Encriptação da informação de autenticação

A informação de autenticação pode ser armazenada, de forma encriptada, no sistema multifuncional, ou pode-se usar informação de acesso existente, por exemplo do Windows Active Directory. Além disso, a autenticação pode ser gerida centralmente através do Enterprise Suite Authentication Manager. Isso garante que nenhuma pessoa sem autorização consegue ler informações de autenticação ou gerir os direitos de acesso.

Reinicialização automática

Caso se esqueceu de fazer logout, o sistema fica normalmente livre para ser utilizado. Por conseguinte todos os sistemas ineo podem ser programados para fazer uma reinicialização automática afim de solicitar a introdução de uma palavra passe após um período específico de inatividade. Isso garante que o sistema volta a um estado seguro caso um utilizador se esqueça de fazer logout quando terminar. A proteção por palavra passe também pode ser usada para limitar o acesso aos documentos no sistema a partir de postos de trabalho remotos. Muitos equipamentos da Develop oferecem a possibilidade de aceder remotamente aos trabalhos de impressão e de digitalização. Esta caraterística pode ser protegida por palavra passe ou completamente desativada.

Bloqueio de acesso não autorizado

Tal como uma caixa multibanco, cada sistema ineo pode ser programado para rejeitar um utilizador que tenta autenticar-se com uma palavra passe errada. Após um determinado número de tentativas erradas, o equipamento bloqueia o acesso por um período definido. Esta função de bloqueio de acesso não autorizado também pode ser aplicada na caixa de utilizador para documentos confidenciais (caixa de impressão segura). Esta caraterística protege o sistema multifuncional contra ataques de força bruta pela introdução de muitas palavras passe num curto espaço de tempo efetuada por ferramentas dos hackers.

Limitação de funcionalidades

Um nível avançado de segurança do utilizador gere a disponibilidade de caraterísticas específicas, permitindo ou priobindo a sua utilização. Um operador ou administrador pode gerir estas caraterísticas como pretendido dentro de qualquer organização. As caraterísticas específicas são:

- Copiar na ineo como função walk-up, incluindo as restrições de cópia apenas em p/b ou apenas em cor ou nem cópia a p/b nem a cores
- Imprimir como função remota através do driver de impressora, incluindo as restrições de impressão apenas em p/b ou apenas em cor ou nem impressão a p/b nem a cores
- Digitalizar a partir da ineo como função walk-up ou remota
- Fax a partir da ineo como função walk-up ou remota
- Caixa de utilizador a partir da ineo como função walk-up ou remota
- Além disso, é possível limitar várias funções às utilizadores individuais. Isso pode ser feito em combinação com os métodos de autenticação mencionados anteriormente.

Informação de registo

A informação de registo para o acesso e utilização dos equipamentos individuais não só permite a deteção imediata de falhas de segurança, mas também facilita o accounting e a atribuição dos custos a utilizadores e departamentos. O administrador pode rever de forma individual cada auditoria e registos de trabalho para as várias funções do equipamento, incluindo a impressão e/ou cópia a p/b e cor, receção e envio de fax, e digitalização. Muitos controladores de impressão nos sistemas Develop contêm registos de trabalho eletrónicos que registam todos os trabalhos de impressão enviados para o equipamento. Além disso, o Job Log Utility da Develop fornece registos eletrónicos de monitorização abrangentes da atividade de utilizador.

Monitorização da conta

A monitorização da conta requer um login de utilizador no equipamento e fornece uma monitorização eficiente a nível de utilizador, grupo e/ou departamental. Todas as cópias monocromáticas e a cores, digitalizações, fax e impressões a p/b e cores podem ser monitorizadas localmente no equipamento ou remotamente através de software da Develop como por exemplo Web Connection, Device Manager e Enterprise Suite Account Manager. Quando logado, as atividades do utilizador são registadas de forma eletrónica num ficheiro de registo dentro do sistema, que pode ser consultado pelo administrador ou operador. Esta caraterística fornece um suporte eficiente para por exemplo os departamento de faturação ou para controlar as atividades de cópia dos funcionários.

Segurança documental & Segurança de dados – Dados e informação confidencial protegida pela Develop

Caso um sistema multifuncional esteja instalado numa área pública, os funcionários, fornecedores ou até visitantes podem ter acesso à informação confidencial. Esta informação pode ficar disponível nas impressões no tabuleiro de saída ou armazenada no disco rígido do sistema. A funcionalidade de segurança abrangente da Develop protege a informação de utilizador e o conteúdo impresso e ajuda a evitar que informação corporativa sensível possa cair nas mãos erradas.

Impressão segura

Os equipamentos de impressão são considerados um risco de segurança que não deve ser subestimado: ao nível mais simples, os documentos que se encontram no tabuleiro de saída podem ser vistos e lidos até por pessoas que passam. Não existe forma mais simples para as pessoas sem autorização obter acesso à informação confidencial. A funcionalidade de impressão segura mantém os documentos confidenciais ao exigir a introdução de uma palavra passe pelo autor do trabalho de impressão como medida de segurança antes de impressão. Os documentos protegidos não podem ser impressos até que a palavra passe definida no driver seja introduzida diretamente no equipamento. Isso garante que tais documentos apenas estejam disponíveis para as pessoas que podem lê-los. Cada palavra passe relacionada ao trabalho de impressão é encriptada. Como proteção adicional, os sistemas ineo podem ser configurados para eliminar todos os trabalhos de impressão segura e não impressos após um período de tempo definido.

A impressão segura também está diponível através da funcionalidade conveniente Touch & Print ou ID & Print. Touch & Print é baseada na autenticação por veias de dedo ou leitor de cartões IC, enquanto ID & Print requer a autenticação de utilizador através do nome de utilizador e palavra passe. Com essas caraterísticas, não é necessário uma identificação adicional de impressão segura e palavra passe; em vez disso a informação de autenticação de utilizador é usada para a identificação de um trabalho de impressão segura armazenado e a libertação do trabalho imediatamente após autenticação no equipamento.

Em alternativa, os trabalhos de impressão podem ser protegidos pela impressão segura na caixa de utilizador. A funcionalidade de caixa de utilizador nos sistemas ineo permite ao utilizador armazenar os seus documentos numa caixa pessoal que apenas estão visíveis após autenticação e apenas acessíveis com uma palavra passe de utilizador adicional. Para poder ter acesso a tais trabalhos de impressão para a sua impressão ou envio por fax, o utilizador tem de introduzir o nome de utilizador e a palavra passe correta.
Ao mesmo tempo as caixas de utilizador protegidas permitem também a receção de fax confidencial.

Encriptação de PDF

O conteúdo de PDFs pode ser encriptado pela encriptação standard de 40- ou 128-bit. PDFs encriptados estão protegidos por uma palavra passe de utilziador que pode conter até 32 caratéres. Como parte da encriptação é possível especificar as permissões para a impressão ou cópia do PDF ou até a edição do seu conteúdo.

Encriptação por Senha Digital

A informação em PDF que é anexada a um email ou enviada para uma pasta FTP ou SMB pode ser encriptada por uma senha digital. A tal encriptação de PDF impossibilita a interceção da informação do PDF. A encriptação por Senha Digital é baseada na encriptação S/MIME e requer uma chave pública para a encriptação e uma chave pessoal para a descriptação.

Assinatura digital

Para evitar a manipulação de PDFs criados num sistema ineo, uma assinatura digital pode ser adicionada ao PDF. Esta monitoriza qualquer alteração efetuada ao PDF após a sua criação. A assinatura digital indica claramente todas as alterações à informação de segurança do PDF. Além da prevenção de manipulação dos documentos, a assinatura digital fornece detalhes acerca da fonte do documento, ajudando a reconhecer se este é segura ou não.

Proteção de cópia

Com a proteção de cópia, que está disponível em certos modelos ineo, uma marca de água de segurança escondida é colocada no documento original durante a sua impressão. A marca de água de segurança pode ter várias frases e/ou padrões. Quando um documento protegido é copiado em qualquer outro sistema, a marca de água de segurança irá aparecer indicando ao destinatário que este documento foi copiado e/ou distribuído sem autorização.

Copy Guard/Password Copy

A característica opcional Copy Guard/Password Copy adiciona uma marca de água de segurança ao original durante a sua impressão para evitar a cópia de documentos. Embora quase invisível no documento original protegido, não é possível copiar este documento. O equipamento está bloqueado para esta operação. A característica de Password Copy pode desativar o copy guard e permite a cópia com a introdução da palavra passe correta no painel do sistema.

Proteção do Disco Rígido

A maioria das impressoras e sistemas multifuncionais tem acesso a discos rígidos e memória que podem possuir muitos gigabytes de informação confidencial, durante períodos longos. As guarda-costas de confiança devem portanto estar disponíveis para garantir a segurança de informação corporativa e sensível. Na Develop as várias caraterísticas sobrepostas e interligadas fornecem esta garantia.

Encriptação do Disco Rígido

A Develop oferece a encriptação do disco rígido para a maioria dos equipamentos multifuncionais. Isto é importante para as empresas que se preocupam com a segurança dos documentos armazenados como informação eletrónica em caixas protegidas com palavra passe no disco rígido do sistema. A informação armazenada pode ser encriptada utilizando o Advanced Encryption Standard (AES) que suporta o tamanho da chave 128-bit. Uma vez que o disco rígido esteja encriptado, a sua informação não pode ser lida até mesmo quando o disco rígido é removido.

Auto eliminação dos dados no Disco Rígido

Uma função de auto-eliminação apaga a informação armazenada no disco rígido interno após um período de tempo definido. Esta caraterística de formatação/eliminação do disco rígido protege a informação sensível armazenada nos discos rígidos dos sistemas ineo. A informação armazenada pode ser eliminada pelo utilizador que guardou o documento pela primeira vez.

Sobrescrever o Disco Rígido

Para uma maior segurança, um operador, administrador ou técnico pode formatar fisicamente o disco rígido, por exemplo quando o sistema precisa de ser realocado. Os discos rígidos podem ser sobrescritos utilizando vários métodos diferentes de acordo com as várias especificações (por exemplo militares). Além disso, os administradores podem programar a ineo para apagar automaticamente todos os dados temporários no disco rígido numa base por trabalho. Se o sobrescrito automático esteja ativo, os trabalhos eliminados manualmente numa caixa de utilizador também serão sobrescritos três vezes.

Disco Rígido protegido por palavra passe

A proteção por palavra passe do disco rígido interno impede a sua remoção não autorizada; a palavra passe está ligada ao equipamento pelo que os dados não estejam acessíveis caso o disco rígido é retirado e instalado em outros equipamentos como por exemplo um PC etc.

Segurança de rede – comunicação de rede segura com Develop

Os equipamentos de escritório da Develop têm como base o conceito de comunicação e de conetividade. Isto está de acordo com as normas de segurança rígidas no que respeita o acesso de utilizador, encriptação de informação e protocolos usados para a transmissão de informação para que pode ter a certeza de que a sua informação chega ao destino desejado de forma segura e fiável.

Autenticação de Utilizador

Além de regular o acesso aos equipamentos de impressão, a autenticação de utilizador também impede o acesso à rede de utilizadores sem autorização. Com esta caraterística, que pode ser configurada para a autenticação na rede ou localmente no equipamento, cada utilizador autorizado tem um ID de utilizador e uma palavra passe exclusiva.

Encriptação por SSL/TLS

A encriptação por SSL e TLS protege a comunicação a partir de e para os equipamentos de impressão, cobrindo ferramentas de administração online, por exemplo as transmissões do Enterprise Server e Active Directory. Este tipo de comunicação impede os ataques "man-in-the-middle" onde o atacante seria capaz de gravar a comunicação de dados.

IPsec

Os equipamentos ineo também suportam IPsec para a encriptação total de qualquer transmissão de dados pela rede a partir de e para o sistema multifuncional. O protocolo de segurança IP encripta toda a comunicação de rede entre a intranet local (servidor, PC) e o próprio equipamento.

Filtragem endereço IP

Um firewall básico interno fornece a filtragem de endereços IP e o controlo de acesso aos protocolos e portas. A filtragem de endereços IP pode ser definida no equipamento: a placa de rede do sistema multifuncional pode ser programada para autorizar apenas o acesso ao equipamento por endereços IP específicos a partir dos PCs.

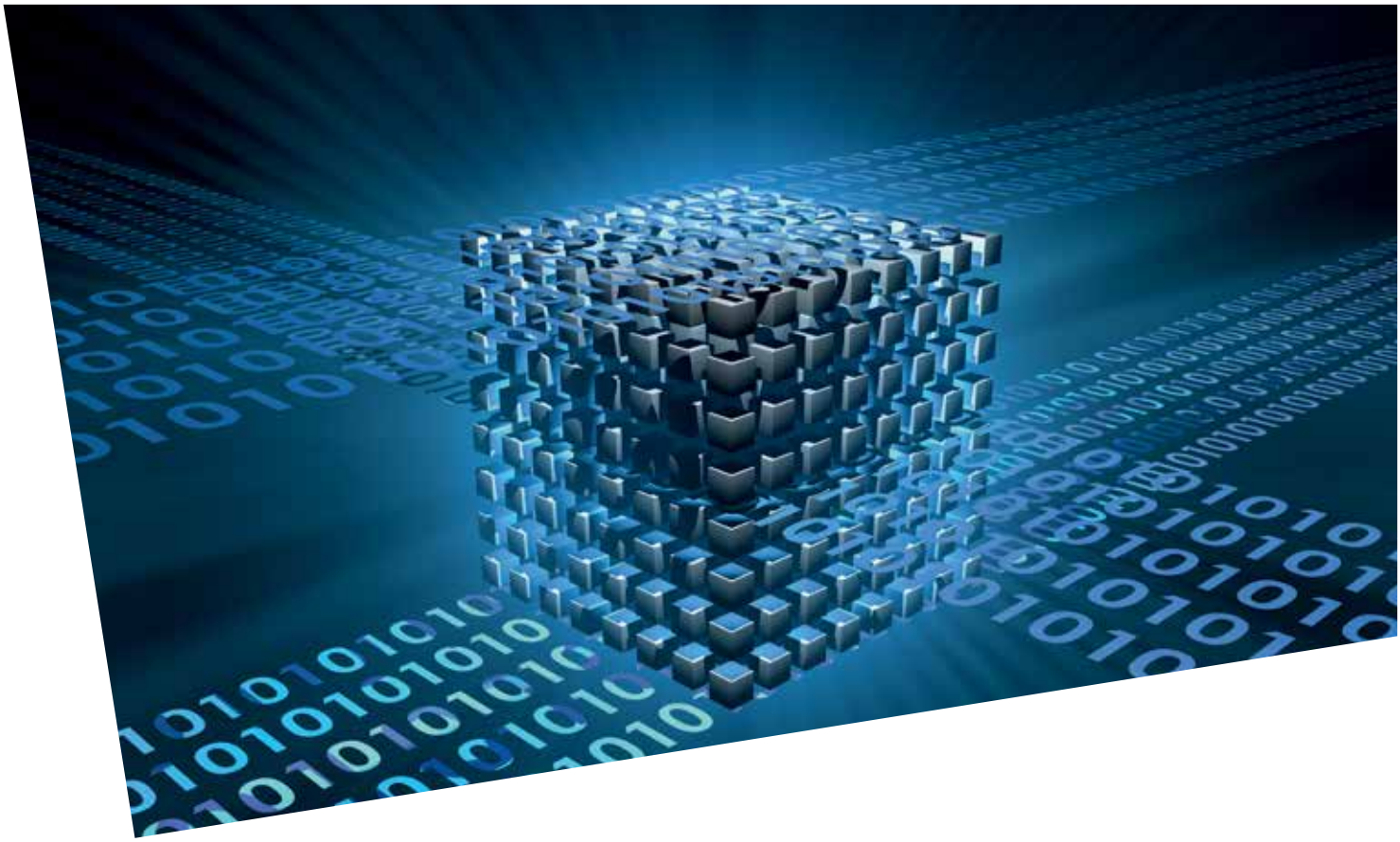
Portas e protocolos protegidos pelo administrador

As portas e os protocolos podem ser abertos, fechados, ativados e desativados através do modo administrador no equipamento ou remotamente através do Web Connection ou Device Manager. Como proteção contra a manipulação sem autorização através das definições de equipamento e de rede, o próprio modo de administrador possui uma palavra passe alfanumérica de 16 dígitos, que só pode ser alterada pelo técnico ou na área de administrador.

Caso seja necessário, uma função de fecho da interface web permite a desativação da interface web, ou seja, Web Connection, para todos os utilizadores. Isto limita o acesso por web para os administradores, fornecendo uma proteção de confiança contra a manipulação das configurações, definições, etc. por pessoas sem autorização.

Autenticação por SMTP

A autenticação por SMTP (Simple Mail Transfer Protocol) fornece uma segurança de email avançada. Quando ativado, o SMTP autorizará o equipamento para enviar emails. Para aqueles clientes que não alojam os seus serviços de email, a utilização de um servidor de mail ISP é possível e suportado pelo equipamento. A autenticação por SMTP é exigido pela AOL e para a prevenção de spam. Para a comunicação segura também é possível combinar a autenticação ou encriptação POP antes de SMTP, APOP, SMTP usando SSL/ TLS.



Encriptação S/MIME

Para proteger a comunicação segura por email a partir do sistema multifuncional para determinados destinatários, o sistema suporta S/MIME (Secure/ Multipurpose Internet Mail Extensions). S/MIME encripta a mensagem e o conteúdo do email com um certificado de segurança.
Os certificados S/MIME ou chaves de encriptação (chave pública) podem ser registados para os endereços email armazenados no livro de endereços do sistema. Os emails encriptados por S/MIME apenas podem ser abertos pelo proprietário da chave de decriptação (chave privada).

Alterar o endereço "De"

Quando a autenticação de utilizador estiver ativada, não é possível alterar o endereço 'De'. Apesar da função 'Alterar Endereço De' estar ativada, o endereço 'De' de um trabalho de scan-para-email será sempre o endereço email do utilizador logado. Esta caraterística evita falsificação e fornece aos administradores pistas de auditoria.

Priobição de Destinos Manuais

Com a função 'Priobição de Destinos Manuais', a introdução direta de um endereço email ou destino de digitalização é impossível. Se esta função estiver ativada, apenas os destinos registados no livro de endereços interno no sistema ou LDAP podem ser utilizados.

Segurança da linha de fax

A segurança avançada da linha de fax é garantida pela conexão fax ineo usando apenas o protocolo de fax para a comunicação – nenhum outro protocolo de comunicação é suportado. Os produtos da Develop bloqueiam quaisquer tentativas de intrusão como ameaças, incluindo intrusões de um protocolo diferente por linhas telefónicas públicas, bem como qualquer tentativa de transmissão de dados que não pode ser descompatada como dados de fax.

Reencaminhamento de fax

O reencaminhamento de fax permite o encaminhamento automático de faxes recebidos para qualquer destino dentro do livro de endereços interno da ineo, incluindo por exemplo endereços email, ou para as caixas de utilizador no disco rígido interno da ineo. O armazenamento de faxes recebidos numa caixa de utilizador é consideravelmente mais seguro, já que não existem faxes impressos no tabuleiro de saída. Este reencaminhamento também poderá tornar a comunicação mais rápida, uma vez que os faxes chegam mais rapidamente ao seu destinatário. Por último, também ajuda a poupar papel – os destinatários podem decidir se a impressão de um fax é realmente necessário.

Controlo de acesso à rede

A maioria dos equipamentos Develop suportam a norma IEE802.11x para o controlo de acesso à redes WANs e LANs. Essas normas garantem uma rede segura ao fechar quaisquer comunicações de rede (e.g. DHCP ou HTTP) a equipamentos sem autorização, exeto os pedidos de autenticação.

Esteja preparado para os riscos de segurança diários!

É importante ficar consciente do facto que, hoje em dia, nenhuma empresa ou organização é imune aos riscos de segurança – as falhas de segurança acontecem em todos os lados, sempre! Mas as empresas prudentes olham para frente e tomam as precauções necessárias antes que seja tarde demais. Eles garantem que a informação confidencial nos discos rígidos e na memória das impressoras, copiadoras e equipamentos multifuncionais não pode pode ser acedida tão facilmente, muito menos manipulada.

Proprietários e gestores das empresas conscientes de segurança certificam-se que a sua rede esteja protegida e que o acesso não autorizado à informação na intranet da empresa esteja barrado. Gestores com consciência também apercebem-se que as impressoras e copiadoras instaladas em toda a empresa podem facilmente originar falhas mais graves de segurança. Caso deixado abandonada no tabuleiro de saída, informação confidencial poderá cair nas mãos erradas e poderia facilmente sair da empresa, por exemplo através das transmissões de scan para email ou de fax. Mas gestores e especialistas de TI prudentes protegem-se contra esses riscos pela limitação viável de acesso aos equipamentos a aqueles autorizados e pela proteção contra os documentos não levantados de qualquer tipo de impressões.

A Develop apoia os esforços dos seus clientes na proteção contra os riscos de segurança pela aplicação de vários recursos de engenharia no desenvolvimento avançado de caraterísticas relacionadas com a segurança nos sistemas e impressoras ineo. A Develop proporciona assim os seus clientes com a tecnologia necessária nos atuais ambientes preocupados com a segurança. Se o cliente esteja preocupado com a intrusão na rede, roubo de informação ou conformidade com os regulamentos, ou quando a questão se concentra na limitação de acesso aos equipamentos ou funcionalidades, a tecnologia ineo da Develop oferece as soluções profissionais para a deteção e prevenção de falhas de segurança. Este é o nível de proteção abrangente que os clientes de todos os setores e entidades públicas esperam hoje em dia.

Resumo caraterísticas de segurança e disponibilidade

Caraterísticas	Sistemas multifuncionais a cores				Sistemas multifunctionais a p/b						Sistemas de impressão		
	ineo +25	ineo +35	ineo +224 +284 +364 +454 +554	ineo +654 +754	D 240F	ineo 36 42	ineo 215	ineo 223 283 363 423	ineo 552 652	ineo 501 601 751	ineo +35P	ineo +353P	ineo 40P
Controlo de Acesso/Segurança de Acesso													
Accounting de cópia/impressão	—	●	●	●	●	●	●	●	●	●	—	●	✂
Restrição de funções (cópia/impressão/digitalização/fax/box/cor)	●**	●	●	●	●	●	—	●	●	●	✂	●	—
Impressão segura (bloquear trabalho)	●	●	●	●	●	●	●	●	●	●	✂	●	✂
Proteção por palavra passe caixas de utilizador	—	—	●	●	●	—	—	●	●	●	—	●	—
Autenticação de Utilizador (ID + palavra passe)	✂	●	●	●	●	●	●	●	●	●	✂	●	✂
Scanner veias dedo	—	—	✂	✂	—	—	—	✂	✂	✂	—	✂	—
Leitor de cartões IC	—	✂	✂	✂	—	✂	—	✂	✂	✂	—	✂	—
Registo de atividade	—	—	●	●	—	—	—	●	●	●	—	●	—
Segurança de dados/Segurança de documentos													
Encriptação de dados (disco rígido)	—	●**	●	●	—	●**	—	●	●	✂	—	✂	—
Sobrescrever dados disco rígido	—	●	●	●	●	●	—	●	●	●	—	●	—
Proteção por palavra passe disco rígido	—	—	●	●	●	—	—	●	●	●	—	●	—
Auto eliminação de dados	—	—	●	●	—	—	—	●	●	●	—	●	—
Segurança de rede													
Filtragem IP	●	●	●	●	●	●	—	●	●	●	●	●	●
Controlo de acesso de portas e protocolos	●	●	●	●	●	●	●**	●	●	●	●	●	●
Encriptação por SSL/TLS (https)	●	●	●	●	●	●	●	●	●	●	●	●	●
Suporte IP sec	●	●	●	●	—	●	—	●	●	●	●	●	●
S/MIME	—	●	●	●	—	●	—	●	●	●	—	—	—
Suporte IEEE 802.1x	●	●	●	●	—	●	—	●	●	●	●	—	●
Segurança de digitalização													
Autenticação de utilizador	—	●	●	●	—	●	—	●	●	●	—	—	—
POP antes de SMTP	●	●	●	●	●	●	●	●	●	●	—	—	—
Autenticação SMTP (SASL)	●	●	●	●	●	●	—	●	●	●	—	—	—
Bloqueamento manual de destinos	—	●	●	●	—	●	—	●	●	●	—	—	—
Outros													
Proteção modo serviço	●	●	●	●	—	●	—	●	●	●	●	●	●
Proteção modo admin	●	●	●	●	●**	●	●	●	●	●	●	●	●
Captura de dados	—	—	●	●	—	—	—	●	●	●	—	●	—
Bloqueamento acesso não autorizado	—	●	●	●	—	●	—	●	●	●	●	●	—
Proteção de cópia por marca de água	—	●	●	●	—	●	—	●	●	●	—	●	—
PDF encriptado	—	●	●	●	●	●	—	●	●	●	—	—	—
Assinatura PDF	—	—	✂	✂	—	—	—	✂	✂	✂	—	—	—
Encriptação PDF por ID digital	—	—	✂	✂	—	—	—	✂	✂	✂	—	—	—
Copy guard/Password copy	—	—	✂	✂	—	—	—	✂	✂	—	—	—	—
Certificação ISO 15408													
ISO 15408 EAL 3 certificado	—	●	●*	●*	—	●*	—	●	●*	●	—	●	—

● = standard ✂ = opcional — = não disponível * em avaliação ** com limitações

Por favor contate o seu parceiro para mais informação.

O seu Parceiro Develop:

Janeiro de 2013

Konica Minolta Business Solutions Portugal
Rua Prof. Henrique de Barros 4-10º B 2685-338 PRIOR VELHO Portugal Tel +351 219 492 000 www.develop.pt