RICOH
imagine. change.

Soluções de segurança da Ricoh

Ajudar a proteger a sua empresa

A cibersegurança é a maior ameaça à sobrevivência e ao sucesso das empresas modernas. As empresas, independentemente do tamanho, estão em risco constante de serem vítimas de ataques prejudiciais como, por exemplo, phishing, DDoS ou ransomware. O custo real destes ataques pode atingir milhões de dólares. Em 2017, o Ponemon Institute concluiu que o custo médio global de uma violação de dados era de 3,62 milhões de dólares. Este custo tenderá a crescer nos próximos anos pois a regulamentação governamental, como o GDPR (Regulamento Geral sobre a Proteção de Dados), procura punir as empresas com multas exorbitantes devido a falhas na segurança dos seus sistemas e dados. Para evitar estas pesadas punições, as empresas devem demonstrar a sua capacidade para proteger os dados.
Esta situação requer uma visão global de todas as vulnerabilidades numa empresa.

Outros fatores que compõem o desafio da cibersegurança para as empresas são a expansão e a digitalização dos locais de trabalho modernos, bem como a explosão nos volumes de dados. Os fluxos de trabalho, frequentemente, propagam-se por dispositivos, redes e geografias. As informações estão mais expostas a riscos quando são movidas numa empresa. Devem permanecer protegidas em todas as etapas do seu percurso. Devido aos riscos de segurança que isto apresenta, as empresas modernas não podem mais funcionar sem protegerem os documentos e os sistemas de gestão de dados. Ao mesmo tempo, as capacidades das impressoras de escritório e dos multifunções aumentaram dez vezes nos últimos anos. Estes equipamentos são agora responsáveis por uma enorme proporção de entrada, saída, transferência e armazenamento dos dados empresariais. Esta situação transforma-os num dos fatores de ameaça mais perigosos, ao qual muitas vezes não é dada a devida atenção nos locais de trabalho atuais.

Embora muitas empresas declarem ter capacidades de segurança, a Ricoh tem vindo a desenvolver, há décadas, soluções e serviços de segurança no local de trabalho. As nossas impressoras, por exemplo, possuem funções de segurança de substituição de dados nos discos rígidos há mais de 20 anos.

A segurança está no DNA de todo o nosso portfólio do local de trabalho digital. Atualmente, temos mais de 4 milhões de produtos de escritório instalados. Cada um desses produtos e cada serviço que implementamos em conjunto com os mesmos possuem capacidades de segurança integradas. Também utilizamos um sistema operativo exclusivo da Ricoh em muitos dos nossos produtos. Este é um componente extremamente importante das nossas defesas de segurança, fornecendo controlo e isolamento das ameaças específicas do sistema operativo, que afetam os sistemas operativos mais comuns.

A Ricoh disponibiliza uma estrutura de serviço e suporte consistente a nível mundial aos seus clientes que garante que as informações contra ameaças são partilhadas e abordadas de forma eficiente. Para além de ter a certificação IEEE 2600 implementada como standard nos nossos equipamentos de impressão, a Ricoh é um membro líder e um autor importante da IEEE Standards Association. A Ricoh também está certificada com ISO 27001 e empenhada em continuar a respeitar este sistema de gestão de segurança da informação. Mantemos o desenvolvimento dos nossos produtos focado nas preocupações de segurança e nos requisitos empresariais dos clientes através de uma série de programas de novação globais orientados para o cliente.

Para satisfazer os exigentes requisitos de boas práticas de cibersegurança eficazes e demonstráveis, a segurança está incluída em todos os produtos e serviços no portfólio da Ricoh por conceção – nunca como solução para um problema ocorrido. Acreditamos que esta visão holística das vulnerabilidades é essencial para a sobrevivência nas empresas modernas.

DESAFIO DA SEGURANÇA DOS CLIENTES

TENDÊNCIAS: À medida que os volumes de dados aumentam, as vulnerabilidades, os ataques e as sanções também aumentam.

Proteger e fortalecer locais de trabalho digitais

A Ricoh procura capacitar e proteger o trabalho digitalizado, em qualquer lugar onde se trabalhe. Numa economia digital moderna, isto significa um valor acrescentado para além da conceção do escritório tradicional em locais de trabalho de vanguarda. Os escritórios e os colaboradores remotos proporcionam às empresas grande flexibilidade e ganhos de produtividade nas operações do dia a dia, uma vez que ajudam as empresas a satisfazer as expectativas e os requisitos de serviços dos clientes.

No entanto, o funcionamento no perímetro da rede implica alguns dos maiores riscos para a segurança das empresas. Os dados que estes colaboradores geram e os dispositivos remotos que utilizam para obter esses dados têm de ser adequadamente seguros. Os colaboradores operam, muitas vezes, através de redes e geografias, complicando ainda mais esta tarefa. De importância crucial é o facto de as regulamentações governamentais, como o Regulamento Geral sobre a Proteção de Dados, obrigarem as empresas a demonstrarem a segurança dos dados durante o seu período de vida útil para não enfrentarem sanções graves. À medida que os locais de trabalho evoluem e adotam fluxos de trabalho digitais, o ciclo de vida dos dados empresariais torna-se, gradualmente, mais complicado. Vamos analisar agora esta situação, fase a fase.

O primeiro passo é a entrada de dados e os dispositivos de captura – um componente vital da defesa de segurança da Ricoh. A partir daqui, os dados devem ser transportados através de redes e armazenados em segurança. Nesta fase, a preservação da integridade dos dados é crucial. Os sistemas Ricoh restringem o acesso dos utilizadores aos dispositivos e às funcionalidades de rede para assegurar que os dados não podem ser manipulados no transporte ou em repouso. Estes serviços incluem controlo do acesso, codificação e proteção contra cópias. A esta fase chamamos de Controlo.

No entanto, depois de guardados, os documentos ficam facilmente acessíveis por parte de quem, na empresa, necessitar deles. A capacidade de obter informações sempre que é necessário e de visualizá-las depende, efetivamente, desta disponibilidade. A análise dos dados é um componente vital do local de trabalho digital fortalecido. Fornece, efetivamente, uma visão de todos os elementos da empresa, desde as vendas até aos RH. As ferramentas da infraestrutura de autorização permitem um acesso seguro e rápido, independentemente da localização do utilizador ou

da escolha do dispositivo. É vital que os protocolos de segurança não prejudiquem a inovação, a funcionalidade ou a prevenção de riscos dos funcionários. A esta fase chamamos Preservação.

Finalmente, estes dados devem ser eliminados de uma forma segura e auditável. Esta fase é essencial tendo em vista a conformidade com os requisitos regulamentares e minimiza a possibilidade do subsequente roubo ou perda. Este processo ocorre, na verdade, ao logo do período de vida útil dos documentos, bem como na sua eliminação final. A impressão de qualquer ficheiro deixa uma imagem latente na unidade de disco rígido das impressoras multifunções que deverá ser substituída para evitar o acesso não autorizado. Os serviços de eliminação de dados da Ricoh incluem a limpeza do disco rígido, a retirada dos dados da memória, a eliminação dos ficheiros não impressos e a eliminação da funcionalidade de fim de sessão para evitar que piratas informáticos compilem informações confidenciais a partir dos rastos que um documento deixa para trás. A esta fase chamamos de Destruição.

Para proteger eficientemente os dados do local de trabalho durante todo este ciclo de vida, a Ricoh utiliza os princípios CID de privacidade e segurança: Confidencialidade, Integridade e Disponibilidade. Estes são os nossos princípios orientadores na conceção dos nossos produtos e soluções para satisfazer as normas e regulamentações necessárias. Esta abordagem permite a inovação e o crescimento do local de trabalho ao mesmo tempo que são mantidos processos eficazes e seguros.

ABORDAGEM DA RICOH RELATIVAMENTE À SEGURANÇA

Desenvolvemos produtos e serviços com base nos princípios CID de privacidade e segurança: confidencialidade, integridade e disponibilidade

A segurança está no nosso DNA. Todos os produtos criados e serviços utilizados pela Ricoh contêm funcionalidades e capacidades de segurança integradas

A Ricoh oferece um conjunto completo de produtos e serviços de segurança para proteger a criação de documentos desde o início até ao fim.

Iremos agora explorar cada fase crucial individualmente: controlo, preservação, destruição e suporte.

QUATRO ETAPAS DA SEGURANÇA DO LOCAL DE TRABALHO DIGITAL

1 CONTROLO

Os controlos eficazes dos dados são cruciais para a manutenção da confidencialidade e integridade dos dados. As informações empresariais são um ativo extremamente importante que tem de ser protegido. Os dispositivos de hardware atuais são terminais de informação que podem funcionar como portas de acesso vulneráveis para as informações empresariais. Por isso, a Ricoh utiliza várias ferramentas de autenticação do utilizador e de gestão de dispositivos para controlar e proteger os dados empresariais. Estas pertencem às definições de dispositivos físicos que permitem e restringem o acesso a determinadas funcionalidades e dados. Limitar o acesso dos colaboradores às informações que circulam através de qualquer impressora multifunções de escritório é um passo crucial de boa prática para manutenção da segurança documental. A fase de controlo também inclui proteção de malware de dispositivo através da abordagem hierarquizada da Ricoh para firmware de dispositivo.

Controlo de cópias não autorizadas

Para proteção contra tentativas de execução de cópias não autorizadas, a Ricoh oferece uma solução elegante para garantir a segurança dos documentos em papel. A função de proteção de cópia imprime ou copia documentos com padrões invisíveis especiais incorporados em segundo plano. Se o documento impresso ou copiado for fotocopiado ou digitalizado, os padrões incorporados ficam visíveis nas cópias. O módulo de proteção contra cópias não autorizadas permite que o multifunções detete os padrões incorporados e substitua a imagem copiada por uma imagem cinzenta, para evitar as fugas de informação. Esta função é útil quando da impressão de informações confidenciais. Restringir a duplicação das informações confidenciais evita este tipo de fuga de informações.

Impressão bloqueada

Um documento recebido de um computador pode ser guardado na unidade de disco rígido do multifunções. Utilizando a função de impressão bloqueada da Ricoh, é especificada uma palavra-passe quando um utilizador envia o documento e essa palavra-passe deve ser introduzida no multifunções antes de o documento ser impresso. Uma vez que o documento será impresso até o proprietário chegar ao equipamento, a impressão bloqueada garante que o documento permanece sob controlo do seu proprietário.

Segurança de captura avançada

O portfólio de soluções de captura avançada da Ricoh oferece vários níveis de encriptação e desencriptação em todos os níveis de processamento, ao longo das etapas do processo de captura. Os administradores podem autorizar o acesso às filas de processamento por início de sessão de utilizador individual ou por credenciais de grupo. Os níveis adicionais de segurança incluem SAML (Security Assertion Markup Language) para uma estrutura Single Sign On (SSO), Personal Identity Verification (PIV) e encriptação Public Key Infrastructure (PKI).

Controlos de autenticação integrados

Os protocolos de acesso aos dispositivos e de autenticação de identidade nos produtos Ricoh podem ser geridos centralmente. Os métodos disponíveis incluem cartão de identificação, número de PIN, início de sessão via rede ou uma combinação multifator dos métodos anteriores. A autenticação multifator melhora a segurança mas pode abrandar os utilizadores mais atarefados. A opção Single Sign On (SSO) é um auxiliar importante pois permite que os utilizadores acedam a um conjunto de dispositivos sem esforço. Além disso, a Autenticação rápida da Ricoh, o software de autenticação baseado na passagem de cartão, está pré-instalada nos nossos equipamentos, oferecendo aos utilizadores uma forma fácil de acederem aos seus documentos. A utilização de um leitor NFC simplifica imenso o processo de início de sessão do utilizador, ao mesmo tempo que protege e controla, de forma eficiente, o acesso ao multifunções. Este tipo de acesso também funciona em conjunto com a definição de permissões dos multifunções existentes para restringir o acesso dos utilizadores às funções do equipamento, conforme determinado pelo cliente.

Streamline NX (SLNX)

O módulo do gestor de dispositivos na plataforma Streamline NX é um software da Ricoh para a gestão e monitorização de equipamentos numa rede. O software permite que os administradores visualizem e configurem as definições dos equipamentos, utilizando modelos pré-fornecidos e parâmetros personalizados. As definições de segurança cruciais incluem ativação/desativação de protocolos, definições de endereço IP, palavras-passe de administradores, endereços de e-mail para alertas, definições de encriptação, entre outras. O SLNX também pode criar um relatório de todas as impressoras que não estão em conformidade com base na política de um cliente.

Proteção contra malware dos dispositivos

A Ricoh tem uma abordagem de três níveis para proteção contra malware nos seus dispositivos. Em primeiro lugar, os dispositivos da Ricoh só podem ser operados utilizando uma linguagem de equipamento ou sistema operativo exclusivo da Ricoh. Em segundo lugar, para prevenir a manipulação maliciosa do software do dispositivo, todas as atualizações do firmware têm de ser escritas e aprovadas exclusivamente nesta linguagem de equipamento Ricoh. Finalmente, todas as atualizações do firmware devem ser assinadas digitalmente pela Ricoh. Utilizando este método de três passos, não é possível carregar firmware não aprovado em dispositivos Ricoh. Desta forma, malware, spyware e vírus são eliminados de modo eficiente.

Segurança dos documentos físicos

As boas práticas de segurança não são sempre complicadas. Os escritórios são locais com muito movimento e a documentação em papel constitui um risco significativo para a empresa, em termos de roubo e de negligência dos funcionários.
A Ricoh disponibiliza várias opções de segurança física adicional para prevenir o acesso não autorizado aos documentos em papel. Por exemplo, o bloqueio das bandejas de papel evita o roubo de documentos confidenciais como, por exemplo, os formulários de receitas médicas num ambiente de cuidados de saúde. A instalação de placas de proteção para todos os cabos também evita a possibilidade de ameaças internas, como a manipulação. Uma solução de desbloqueio seguro do documento (print-to-me) garante que os documentos só são impressos quando o proprietário está presente, de forma a eliminar o risco de impressões sem recolha.

2 PRESERVAÇÃO

De acordo com os requisitos regulamentares novos e existentes, as empresas devem garantir a confidencialidade das informações, para que não sejam roubadas ou divulgadas, e a sua integridade contínua para que não seja alterada. Para tal, as empresas devem restringir o acesso aos documentos confidenciais. Isto evita a modificação não autorizada e a falsificação. Também funciona como proteção de ameaças específicas ou oportunistas dentro da empresa.

O trabalho móvel adiciona complexidade a qualquer cenário de cibersegurança. Necessitam de estar implementadas medidas de segurança adicionais para que possa ser efetuada a partilha de ficheiros a partir de qualquer localização. Esses ficheiros devem estar tão protegidos em trânsito através das redes e entre dispositivos como estão em armazenamento. A tecnologia de encriptação forte pode, efetivamente, seguir e proteger os dados durante todo o seu ciclo de vida útil. Isto aplica-se, naturalmente, aos documentos mas estende-se a elementos de segurança cruciais como, por exemplo, palavras-passe guardadas, definição de macro e livros de endereços. Com a encriptação ativada, mesmo que os piratas informáticos consigam aceder à sua rede terão dificuldade em extrair alguma informação útil, preservando a sua integridade mesmo na eventualidade de violação.

O tempo de operacionalidade contínua é fundamental para muitas indústrias. Os eventos imprevistos, como desastres naturais, representam, portanto, um risco direto para as empresas. Os documentos em papel são particularmente vulneráveis neste cenário. A utilização de um repositório seguro e baseado em cloud para documentos digitalizados proporciona resistência crucial contra os desastres naturais ou causados pelo homem. No entanto, devem ser dados passos de segurança apropriados para preservar estes dados digitais.

Codificação de dados essenciais

Para proteger informações que circulam entre dispositivos, a encriptação pode ser ativada para quaisquer dados transferidos para ou residentes no disco rígido de um multifunções da Ricoh. As opções de software integradas proporcionam uma encriptação completa para os ficheiros digitalizados e impressos através da chave PKI (Public Key Infrastructure) do utilizador. Esta funcionalidade protege contra os ataques MITM (man in the middle) no ambiente de TI do cliente.

Para uma maior segurança, os dados impressos são também continuamente substituídos pelo DOSS (Data Overwrite Security System) da Ricoh, que iremos discutir com mais detalhe posteriormente na 'fase de destruição' do ciclo de vida dos dados.

Proteção de bios e sistema operativo

Os multifunções da Ricoh utilizam um TPM (Trusted Platform Module) que consiste num módulo de segurança de hardware à prova de intromissão. O TPM executa funções de criptografia e guarda, de forma segura, os dados criptográficos. A Ricoh utiliza o TPM para guardar a chave de encriptação de raiz que protege a chave de encriptação dos dados do disco rígido e o certificado digital dos multifunções. Também permite que os administradores executem uma operação de arranque segura, validando a autenticidade do firmware dos multifunções antes de permitir o seu funcionamento.

Validação do firmware

A chave de raiz e as funções de criptografia estão sempre contidas no TPM e não podem ser alteradas fora da firewall, evitando a utilização indevida ou manipulação dos nossos produtos. Este processo proporciona uma validação de nível elevado do firmware do multifunções, identidade do dispositivo e segurança do disco rígido. Este é outro bom exemplo de como os produtos multifunções da Ricoh são concebidos a pensar nos interesses de segurança dos clientes da Ricoh.

Gestão de palavras-passe

Os equipamentos da Ricoh podem ser configurados com vários utilizadores com permissões de administrador, cada um com papéis diferentes e palavras-passe distintas. As palavras-passe para estes utilizadores podem ser configuradas remotamente utilizando ferramentas de administração baseadas em web e verificadas regularmente. Isto permite a 'segregação de deveres', que é um requisito presente em várias regulamentações empresariais.

Restrição do acesso de utilizadores

A ferramenta de gestão de utilizadores da Ricoh permite que os administradores do sistema restrinjam os privilégios de acesso dos utilizadores. Por exemplo, o administrador pode configurar privilégios para disponibilizar a determinados utilizadores acesso a um livro de endereços registados no multifunções. Este procedimento bloqueia o acesso não autorizado às informações pessoais e registos guardados nos equipamentos de escritório.

Função de bloqueio de utilizadores

Quando são consecutivamente introduzidas palavras-passe erradas durante o procedimento de início de sessão, o multifunções da Ricoh pode avaliar se alguém está a tentar decifrar a palavra-passe. Isto aciona a função de bloqueio que impede o acesso ao nome de utilizador em questão. O nome de utilizador bloqueado não pode ser autenticado, mesmo se posteriormente combinado com a palavra-passe correta. O bloqueio só pode ser cancelado passado um determinado período de tempo ou pelo administrador impedindo, efetivamente, a ação dos pretensos piratas informáticos.

3 DESTRUIÇÃO

A eliminação segura dos dados é uma parte essencial de qualquer defesa da cibersegurança abrangente. É fácil cair na armadilha de assumir que as responsabilidades da empresa terminam quando os dados saem da organização. No entanto, muitas regulamentações estipulam que a destruição dos dados deve ser um processo abrangente, eliminando qualquer risco de roubo ou utilização indevida subsequente. Até esta situação ser provada, as obrigações de uma empresa em relação aos seus dados não estão terminadas.

Os equipamentos de escritório em fim de vida útil e devolvidos representam, frequentemente, um risco não reconhecido para as informações empresariais. A Ricoh disponibiliza um serviço certificado e auditável para remoção dos dados destas impressoras em fim de vida. Isto inclui material ignorado como, por exemplo, as definições de rede guardadas, os dados de utilizador, os dados do disco rígido ou mesmo os autocolantes deixados no equipamento. Qualquer falha deste tipo representa um risco significativo para as empresas verem expostas informações pessoais e empresariais que sejam confidenciais. Mas, para ser mantida uma conformidade regulamentar, este processo deve também desenvolver-se de forma constante ao longo da vida útil de um dispositivo. Isto garante que as empresas tenham um grau máximo de controlo sobre os dados que estão sob a sua responsabilidade.

Substituição da imagem: DOSS (Data Overwrite Security System)

As unidades de disco rígido dos multifunções funcionam eficientemente, armazenando as imagens latentes dos dados dos documentos em memória para processamento do trabalho. O DOSS da Ricoh garante que as imagens são constantemente substituídas antes de o trabalho seguinte começar. Deste modo, se alguém tiver acedido maliciosamente à unidade de disco rígido, não conseguirá ter acesso aos vestígios de quaisquer dados deixados para trás dos trabalhos anteriores. Na Ricoh orgulhamo-nos de ter disponibilizado esta excecional medida de segurança há mais de 20 anos.

Serviço de limpeza de fim de vida útil

A Ricoh disponibiliza um serviço de limpeza completa dos dados, um serviço de fim de vida útil para multifunções e impressoras que tenham todos os módulos de memória e armazenamento de disco no equipamento apagados de forma a não ser possível a sua recuperação, utilizando soluções de segurança certificadas pela indústria. Os IT Services da Ricoh também disponibilizam um serviço completo de deposição de equipamentos, que inclui vários níveis de serviços certificados de limpeza de dados.

Substituição do disco rígido e armazenamento amovível

A Ricoh também disponibiliza um serviço de eliminação da unidade de disco rígido que permite que os clientes mantenham as suas unidades de disco rígido – substituindo-as por unidades novas e vazias quando o equipamento é devolvido no final do contrato. Isto garante às empresas um controlo completo e demonstrável relativamente ao seu ambiente de dados.

4 SUPORTE

À medida que as empresas crescem, o número de ligações entre dispositivos e redes inevitavelmente também cresce. As empresas necessitam de estratégias para garantir que este crescimento da infraestrutura não representa um risco de segurança. Devem estar cientes dos pontos fracos existentes nos seus sistemas, tomando medidas preventivas contra os ataques específicos e oportunistas.

Frequentemente, é necessário conhecimento especializado em segurança de TI para analisar a infraestrutura de uma empresa e identificar estas vulnerabilidades. Para muitas empresas, a manutenção de pessoal interno de TI com os conhecimentos necessários para gerirem o ambiente de cibersegurança não é uma opção. Os custos e ineficiências desta abordagem conduzem, com frequência, as empresas a uma situação perigosa por não tomarem medidas.

O serviço de suporte de TI da Ricoh disponibiliza serviços de obtenção e configuração de TI, bem como monitorização remota, Service Desk e capacidades de gestão de transições para suporte adicional do processo de cibersegurança. A cibersegurança depende da existência de um entendimento global dos riscos empresariais. A SIRT (Security Incident Response Team) da Ricoh garante que as informações vitais contra ameaças são partilhadas com os clientes em todo o mundo e que respostas eficazes podem ser coordenadas imediatamente.

Avaliação da segurança da infraestrutura

A funcionalidade de gestor de dispositivos SLNX (Streamline NX) da Ricoh foi concebida para executar uma função preciosa de auditoria de políticas de segurança. O SLNX disponibiliza uma funcionalidade que permite que os gestores de TI configurem dispositivos com base nas políticas de uma empresa, distribuam estas definições e analisem as definições utilizando um relatório intuitivo. O SLNX também pode alertar a equipa de gestão quando um dispositivo não está em conformidade com a política da empresa.

Otimização da segurança de impressão

A Ricoh disponibiliza um serviço completo de PSO (Print Security Optimisation) juntamente com serviços de gestão e consultadoria profissionais para identificar falhas de segurança relacionadas com os equipamentos. Esta é uma ferramenta baseada na web com um assistente gráfico que disponibiliza uma visão do estado atual e permite que a Ricoh ofereça recomendações de produtos com o objetivo de redução do risco.

PSIRT (Product Security Incident Response Team)

A resposta ativa da Ricoh às novas ameaças e o desenvolvimento de contramedidas eficazes são geridos pela PSIRT (Product Security Incident Response Team) da Ricoh. Este é um programa que a Ricoh utiliza para garantir que o nosso conjunto de produtos (hardware e software) é continuamente atualizado e protegido contra as mais recentes ameaças e vulnerabilidades identificadas. Isto ajuda a manter, de forma consistente, um nível elevado de serviço numa escala global e a minimizar o impacto dos problemas de vulnerabilidade nos produtos Ricoh.

Documentação de suporte

A preparação e a formação são um elemento crucial de qualquer configuração de cibersegurança. A documentação de backup, os manuais de utilizador, os documentos técnicos de segurança e formação devem ser disponibilizados ao cliente. O mesmo acontece com muitos elementos do ambiente de cibersegurança, a conformidade demonstrável é crucial e esta documentação tem um papel-chave para garantir os resultados financeiros de uma empresa.

COMO PODE A RICOH AJUDAR?

A posição exclusiva da Ricoh em disponibilizar soluções de segurança líderes na indústria em todo o ambiente de TI e de impressão é baseado, em parte, na manutenção de um entendimento forte sobre as condições de mercado em constante alteração e no ajuste em relação à nossa trajetória. As nossas soluções estão concebidas para proteger todas as informações no seu ciclo de vida útil completo e para colocar em prática as quatro áreas de segurança dos dados discutidas neste relatório.

Temos especialistas na matéria responsáveis por analisar as necessidades do mercado, incluindo os requisitos específicos da indústria para os quais podem ser criadas novas soluções ou podem ser personalizadas as soluções existentes.

Também estamos empenhados em desenvolver a nossa capacidade interna para criar e desenvolver soluções centradas na segurança.
Para isso, criámos equipas dedicadas na nossa organização de desenvolvimento de serviço focadas em desenvolver novos serviços de gestão de risco de acordo com a nova regulamentação governamental, assim como serviços de cibersegurança.

Autenticação e autorização de utilizadores

- Impressão bloqueada
- Software integrado standard para autenticação
- Autenticação de utilizadores/restrição de acesso
- Single Sign-On
- Vários papéis de administrador
- Proteção com palavra-passe de PDF (palavra-passe para documentos digitalizados)
- Proteção contra cópias não autorizadas
- Controlo de acesso baseado em intervalo de IP
- Gestão segura de equipamentos e impressão
- Suporte de PKI (Public Key Infrastructure)/SmartCard
- Impressão segura (print2me/impressão bloqueada)

Proteção contra malware dos dispositivos

- Servidores
- Não/menos suscetível para malware
- SOP – versão preparada de Android
- Versão exclusiva da Ricoh do sistema operativo do equipamento (linguagem de controlo do equipamento) para multifunções
- Abordagem de 3 níveis – assinatura digital, download através da ferramenta Ricoh, necessidade de escrever na linguagem de controlo específica

Eliminação do disco rígido

- Eliminação do disco rígido, substituição da imagem,
- Serviço de limpeza completa dos dados
- Serviço de fim de vida útil: destruição dos dados nos módulos de memória, armazenamento

Gestão de dispositivos

- Definição de quotas/limite de contas
- DMNX – painel simples de auditoria de segurança transparente, gestão de palavras-passe, monitorização, alertas

Proteção de bios e sistema operativo

- Arranque seguro utilizando TPM (Trusted Platform Module)

Substituição de imagem e suporte de armazenamento amovível

- DOSS (Disk Overwrite Security System)
- Unidade de disco rígido amovível

Encriptação de dados

- Encriptação do disco rígido via TPM
- Chaves de encriptação via TPM
- Encriptação completa dos ficheiros de impressão e digitalização utilizando a chave PKI
- Disco rígido com certificação FIPS (Federal Information Processing Standards)
- Encriptação completa para impressão
- Encriptação completa para digitalização

Atualizações de firmware e gestão de palavras-passe

- Auditoria remota de palavras-passe
- Função de bloqueio de utilizadores
- Validação do firmware

Conformidade com as normas da indústria

- Certificação ISO 27001
- Certificação IEEE 2600.2 para produtos selecionados
- Certificação ISO 15408 para produtos selecionados
- Documentação e formação de segurança

NÍVEIS DE ABORDAGEM DA SEGURANÇA DE DISPOSITIVOS RICOH

Não há dúvidas de que o papel do fornecedor de multifunções evoluiu para além do fornecimento transacional e unidimensional do hardware para a gestão concreta dos dados. As capacidades dos multifunções expandem agora a captura de informações a partir de entradas multicanal até à classificação dos dados capturados e integração no fluxo de trabalho e à sua análise e armazenamento seguro. Nesta teia complexa de normas rigorosas do ponto de vista regulamentar e requisitos de retenção – juntamente com ameaças internas e externas que colocam os registos em risco de perda, destruição ou tentativa de utilização indevida – fazemos uma abordagem em níveis para a segurança dos dispositivos de modo a garantir que o seu multifunções e os sistemas que lhe estão ligados proporcionam a melhor proteção possível.

1. O dispositivo

No centro de qualquer modelo Ricoh temos o dispositivo. Estes são concebidos, fabricados e implementados com a segurança como um requisito essencial. O sistema operativo exclusivo da Ricoh não partilha vulnerabilidades presentes em muitos sistemas operativos disponíveis no mercado e os nossos dispositivos têm a certificação IEEE2600.2 como standard. A encriptação do disco rígido e a segurança de substituição no disco garantem que os dados que estão a ser processados permanecem confidenciais.

2. O Smart Operation Panel (SOP) disponibiliza o interface de utilizador

De modo semelhante aos multifunções, o SOP utiliza um sistema operativo exclusivo da Ricoh. Não são instalados quaisquer componentes desnecessários e o acesso a raiz não está disponível. A Ricoh trabalhou arduamente para garantir que a segurança do dispositivo não seria enfraquecida pela introdução do SOP.

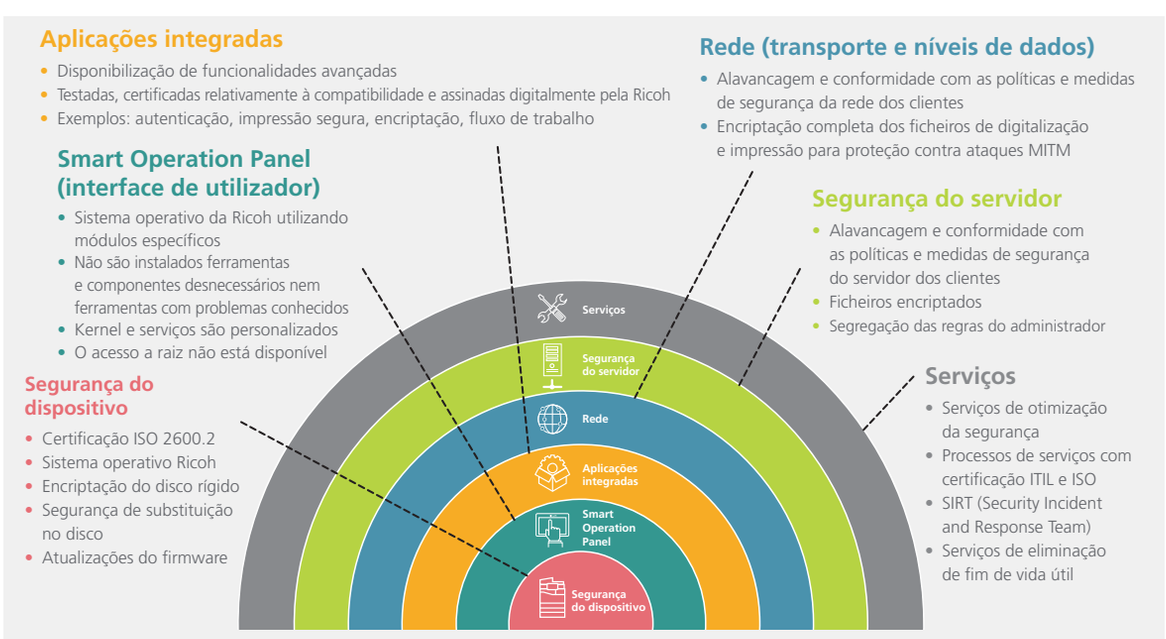
3. Smart Apps

Estas podem ser integradas no SOP proporcionando funcionalidades adicionais aos utilizadores, incluindo fluxo de trabalho e captura de dados. Algumas aplicações disponibilizam funcionalidades de segurança essenciais. Estas incluem capacidade de impressão, acesso por cartão e encriptação. As aplicações são desenvolvidas pela Ricoh ou por membros do Ricoh Developer Programme e todas as aplicações devem passar os testes de Compatibilidade da Ricoh e serem assinadas digitalmente antes de poderem executar o SOP.

4. Rede e servidores

Independentemente de quem gere a infraestrutura de TI, a Ricoh garante que os nossos produtos e serviços estão em conformidade com as suas políticas de segurança de TI e rede. A encriptação completa dos ficheiros de impressão e digitalização, encriptação dos dados nos servidores e segregação dos deveres do administrador são técnicas utilizadas para proteção contra ataque MITM ou "trabalhos internos".

A nossa oferta inclui uma gama completa de serviços integrados de segurança. Isto inclui serviços de gestão e consultadoria para ajudar os clientes e monitorizarem, otimizarem e gerirem a segurança dos seus documentos e informações. Também temos uma gama de serviços de fim de vida para garantir que a RAM e o disco rígido dos equipamentos do cliente retirados de funcionamento são limpos antes da eliminação.



COMO A RICOH PROTEGE O LOCAL DE TRABALHO DIGITAL

Os nossos clientes têm várias preocupações de segurança, todas sustentadas pela verdade empresarial de que, à medida que os volumes de dados aumentam, as vulnerabilidades, os ataques e as sanções também aumentam. Manter a informação confidencial, protegida e impossível de falsificar é uma luta constante. Por exemplo, na Ricoh impedimos cerca de 8 mil milhões de ataques da firewall por mês. Há dezenas de milhares de normas sobre informação confidencial a nível industrial nacional e mundial, e as empresas devem ser capazes de demonstrar o cumprimento de cada uma delas. Compreensivelmente, as empresas de todas as dimensões procuram um parceiro em que possam confiar – um que possa ajudá-las a permanecer em segurança através de um portfólio que abranja todo o local de trabalho digital.

A Ricoh desenvolveu uma vasta gama de soluções para mitigar os vários riscos enfrentados pelas empresas. Como o panorama de ameaça à segurança das informações evolui rapidamente, a Ricoh recorre aos seus programas de 'voz do cliente' para desenvolvimento adicional e fornecimento dos nossos serviços.

Os nossos conselhos consultivos de clientes funcionam como importantes grupos de foco estratégico. Utilizamos estes grupos para obter um melhor entendimento das tendências, catalisadores e prioridades que definem as empresas dos nossos clientes. As nossas conferências consultivas de tecnologia proporcionam o conhecimento vital de decisores-chave. As equipas de engenharia e de R&D da Ricoh utilizam estas conferências para obterem um feedback valioso dos clientes sobre ideias, conceitos e protótipos. Por fim, a Ricoh colabora com clientes individuais para desenvolver novas e avançadas funcionalidades de segurança para os clientes dos mercados verticais e gerais. Esta abordagem orientada para o cliente ajuda-nos a validar o nosso plano de lançamento de produtos e ajuda os nossos clientes a beneficiarem de uma rede global de serviços e suporte.

O local de trabalho digital moderno deve ser tão dinâmico como as ameaças cibernéticas que ele enfrenta e tão flexível como as práticas de trabalho que nele existem. É por isso que acreditamos que a cibersegurança deve funcionar na perfeição em qualquer tecnologia para que os nossos clientes a escolham para o seu local de trabalho. O nosso compromisso para com a norma ISO 27001 em toda a nossa organização e a certificação IEEE 2600 nos nossos produtos, juntamente com o sistema operativo exclusivo da Ricoh que neles utilizamos, significam que os controlos das boas práticas de segurança estão ativos, independentemente do modo que escolher para estruturar e fazer crescer a sua empresa.

Uma combinação de ameaças de segurança, requisitos legislativos e complexas normas da indústria significa que o potencial de danos reputacionais e fiscais dos riscos cibernéticos nunca foi tão grande. Agora chegou o momento de trabalhar com um parceiro de confiança para ajudá-lo a proteger os ativos mais vulneráveis da sua empresa e as suas ambições futuras.

RICOH
imagine. change.

www.ricoh.pt