Lista de verificação relativa ao cumprimento da segurança

O Regulamento Geral sobre a Proteção de Dados da EU exige que as empresas implementem medidas técnicas e organizativas, a fim de proteger informações pessoais e, potencialmente, notificar as pessoas e as autoridades afetadas na eventualidade de ocorrer uma falha de segurança que envolva dados pessoais.

Isto representa um desafio para as empresas, dado que têm de encontrar o tempo e os recursos necessários para cumprir o novo regulamento.

Contudo, se não dispuserem de mais do que uma simples firewall para proteção contra ataques, poderão sofrer ataques à segurança e incorrer em multas que ascendem a milhões de euros. Tendo em conta que todas as empresas poderão sofrer ataques à segurança em determinado momento, é essencial identificar quando tal ocorre e solucionar o sucedido assim que possível com os produtos, processos e ferramentas certos.

Esta lista de verificação é um recurso prático para aqueles que procuram melhorar a respetiva segurança das TI e evitar as consequências dispendiosas de um ataque à segurança. Começando pelo básico, analise a lista para maximizar os níveis de segurança, e pode ter a certeza de que os terminais das suas impressoras estarão seguros e em conformidade com os requisitos do RGPD.

Uma lista útil para proteger dispositivos terminais na sua rede.

Nível de segurança básico

- Adquirir apenas dispositivos que incorporem proteção contra malware e discos rígidos encriptados.
- Atualizar o firmware, especialmente versões com correções ou patches de segurança críticos – tal como quando atualiza as aplicações no seu smartphone.
- Configurar as interfaces do dispositivo e bloquear protocolos, como o FTP e o Telnet, os quais não são necessários para as suas aplicações.
- Analisar novos dispositivos e fechar portas ou protocolos que não estejam atualmente em utilização e que podem disponibilizar acesso a intrusos.
- Aplicar palavras-passe administrativas únicas a cada dispositivo.
- Bloquear o painel frontal para desativar o acesso a funcionalidades de administração.
- Encriptar os dados de e para dispositivos.
- Definir procedimentos de eliminação de dados antigos em discos rígidos – especialmente em impressoras que está a trocar.

Assim que estes passos tiverem sido executados, avance para o nível de segurança seguinte.

Nível de segurança médio

- Integrar os dados de registo dos sistemas de impressoras na sua ferramenta SIEM para monitorizar, de forma mais exaustiva, a rede à procura de ameaças. Para os novos regulamentos de conformidade, a visibilidade é fundamental para cumprir os requisitos de comunicação de incidentes.
- Aplicar a autenticação de utilizador na impressora, para saber quem copia, digitaliza e envia faxes a partir do dispositivo. Esta informação é útil para realizar uma investigação detalhada após a ocorrência do incidente.
- Aplicar a impressão *pull-print* para evitar que informações confidenciais sejam esquecidas. Isto também é benéfico para a sua política de preservação do meio ambiente, já que reduz a quantidade de impressões desnecessárias.

Assim que estes passos tiverem sido executados, avance para o nível de segurança final.

Nível de segurança avançado

- Configurar a monitorização dos trabalhos de impressão e os relatórios de utilização/atividade.
- Configurar e aplicar automaticamente regras relativas a quem pode aceder e usar determinadas impressoras, bem como o motivo da respetiva utilização com autorização baseada na função.
- Aplicar certificados digitais únicos a cada impressora, tal como em qualquer outro dispositivo ligado à Internet na sua rede.
- Aplicar uma solução de impressão móvel para encriptação de dados, acesso de dispositivo na rede, autenticação e monitorização de utilizador

4AA7-1093PTE