LISTA DE VERIFICAÇÃO DE SEGURANÇA DIGITAL

A segurança de dados tem várias facetas. Com o aumento do número de dispositivos conectados em casa ou no trabalho, ficou mais fácil para que criminosos digitais explorem práticas de segurança fracas em qualquer ponto da rede e tenham acesso a dados críticos.

Como usar esta lista de verificação
- Cada caixa marcada equivale a um ponto.
- Marque os itens que foram implementados, e depois calcule seus pontos em cada seção..

A Defesa do perímetro / Roteador

TOTAL DE PONTOS /14

Segurança do sistema

- ☐ 01. Utilização de uma conta de administrador customizada e desabilitação das contas padrão “admin” e “guest”
- ☐ 02. Habilitação de verificação em duas etapas
- ☐ 03. Mudança das portas padrão do sistema para novas portas customizadas
- ☐ 04. Habilitação de IP Auto Block contra ataques de força bruta
- ☐ 05. Habilitação de HTTPS para serviços com certificado SSL válido
- ☐ 06. Habilitação de notificações de e-mail, SMS ou push sobre eventos críticos
- ☐ 07. Habilitação de atualização automática do firmware do roteador e todos os databases de segurança

Segurança da Rede

- ☐ 08. Os dispositivos acessam em casa ou no escritório por meio de uma VPN
- ☐ 09. Habilitação de serviço para bloquear domínios e endereços de IP maliciosos
- ☐ 10. Habilitação de Threat Prevention
- ☐ 11. Habilitação de criptografia DNS over HTTPs para prevenir sequestro de DNS
- ☐ 12. Habilitação de regras GeoIP Firewall
- ☐ 13. Habilitação de filtros Mac e lista branca de dispositivos conhecidos para uso de Wi-Fi
- ☐ 14. Habilitação de relatórios de tráfego programados regularmente para monitorar o uso da rede

B Proteção de Endpoint / NAS

TOTAL DE PONTOS /12

- ☐ 01. Utilização de uma conta de administrador customizada e desabilitação das contas padrão “admin” e “guest”
- ☐ 02. Habilitação de verificação em duas etapas
- ☐ 03. Aplicação de regras de segurança de senha a todos os usuários
- ☐ 04. Restrição a privilégios de acesso de usuários apenas para pastas e serviços necessários
- ☐ 05. Mudança das portas padrão do sistema, por exemplo, porta 5000/5001 para a interface de gestão DSM para novas portas customizadas
- ☐ 06. Se o encaminhamento de portas é habilitado para sua NAS, utilize portas públicas no roteador ao invés de portas bem conhecidas (por exemplo, 5000/5001)
- ☐ 07. Habilitação de IP Auto Block contra ataques de força bruta
- ☐ 08. Habilitação de HTTPS para serviços executando em SRM com certificado SSL válido
- ☐ 09. Habilitação de notificações de e-mail, SMS ou push sobre eventos críticos
- ☐ 10. Habilitação de atualização automática do DSM
- ☐ 11. Execução de Security Advisor regularmente para buscar vulnerabilidades do sistema e identificar malware
- ☐ 12. Instalação de pacote de antivírus e conduzir escaneamento regularmente

C Proteção de Endpoint / Computadores & dispositivos móveis

TOTAL DE PONTOS /4

- ☐ 01. O sistema operacional é mantido atualizado
- ☐ 02. Execução de um software antivírus confiável com escaneamentos regulares
- ☐ 03. Habilitação do Remote Desktop Protocol (RDP) somente quando o acesso remoto é absolutamente necessário, protegendo contra ataques que exploram este protocolo
- ☐ 04. Ao utilizar Wi-Fi pública, sempre fazer criptografia da conexão utilizando uma VPN

D Proteção de Endpoint / Dispositivos IoT

TOTAL DE PONTOS /4

- ☐ 01. Utilização de senha forte
- ☐ 02. Bloqueio de dispositivos (por exemplo, câmeras de IP, impressoras, telefones, etc.) impedindo o acesso à internet exceto quando o dispositivo requer comunicação com o servidor para funcionar
- ☐ 03. Conexão de dispositivos IoT à rede de convidado e separá-los de dispositivos de usuários como computadores, smartphones e NAS, evitando que um dispositivo IoT seja sequestrado e ataque outros dispositivos na mesma rede
- ☐ 04. Bloqueio imediato de dispositivo se apresentar sinais de atividades suspeitas, investigação dos incidentes e reset/reinstalação do dispositivo, se necessário

E Backup de dados

TOTAL DE PONTOS /10

Computadores

- ☐ 01. Habilitação do Synology Drive para fazer backup de arquivos e pastas importantes
- ☐ 02. Uso de Active Backup for Business para fazer backup de todo o sistema

NAS

- ☐ 03. Habilitação de Hyper Backup para fazer backup de pastas compartilhadas, LUNs e configurações de sistema/pacote
- ☐ 04. Configuração de limite de alerta no Hyper Backup para mudanças de arquivos entre duas versões de backup, de forma a notificar automaticamente qualquer comportamento incomum e evitar que todas as versões intactas sejam sobrescritas
- ☐ 05. Habilitação de Snapshot Replication para fazer instantâneos de pastas compartilhadas importantes
- ☐ 06. Habilitação de Cloud Sync para fazer backup continuamente de arquivos e pastas para um provedor de nuvem público seguro como o Synology C2 Backup

Dispositivos externos (por exemplo, USB drives)

- ☐ 07. Utilização de USB Copy para fazer backup de todos os dispositivos externos para a NAS e fazer a gestão de arquivos em um só lugar

Execução de Backup

- ☐ 08. Manutenção de ao menos uma cópia offsite para recuperação de desastre
- ☐ 09. Agendamento de todas as tarefas de backup para execução automática
- ☐ 10. Depois de fazer a configuração de uma tarefa de backup, testar imediatamente e verificar se é possível restaurar os dados a partir da cópia de backup, e repetir o teste regularmente para garantir que sempre é possível executar uma restauração completa quando houver acidentes