



Prime

**ISF – CONTROLE DE ACESSO
A SISTEMAS E ENDPOINT**

Dispositivos Endpoints

O que é um endpoint de segurança?

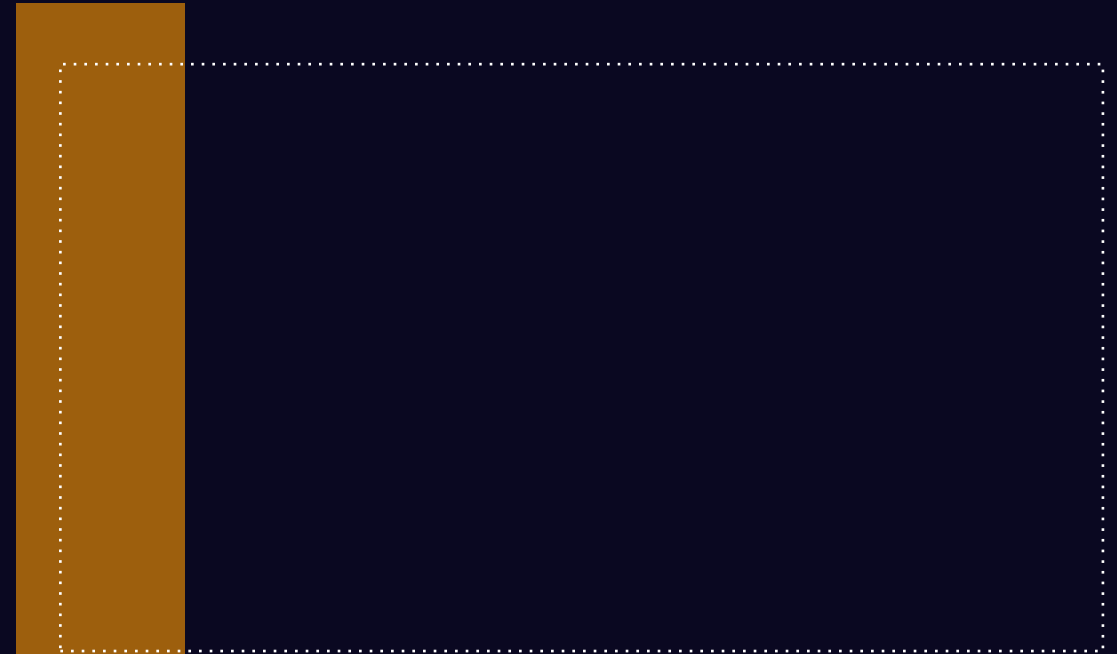


- Uma extremidade de um canal de comunicação;
- Chamado também de dispositivo terminal;
- Pode ser um celular, laptop, notebook;
- Diferente de endpoint de comunicação, como uma API ou protocolos, como TCP.

Proteção de endpoint



- Proteger um endpoint é estender o perímetro de segurança dos dispositivos que estão se conectando à rede;
- Soluções de proteção de endpoint:
 - ✓ Antivírus/antimalware;
 - ✓ Soluções de detecção de intrusão;
 - ✓ Soluções de prevenção de perda de dados;
 - ✓ Firewalls.
- Nem todos os endpoints são iguais, então as soluções devem ser adaptadas.



Controle: Dispositivos Endpoint do Usuário



Objetivo:

Proteger as informações contra os riscos introduzidos pelo uso de dispositivos de Endpoint do usuário.

O podemos fazer para proteger as informações de endpoints?



- Construir uma política de Dispositivos Endpoint do Usuário;
- Definir as responsabilidades dos usuários;
- Quando permitido o uso do BYOD, fornecer orientações neste controle;
- Lidar com a proteção das conexões sem fio.

Considerações sobre Dispositivos Endpoint do Usuário



Considerações:

- O nível de controle depende se o endpoint é usado dentro ou fora da organização;
- Considerar a largura da banda para backup do endpoint;
- Algumas portas USB, como USB-C, não podem ser desativadas, pois são usadas para fornecimento de energia ou saída de exibição.

Política de Dispositivos

Endpoint do Usuário

O que deve constar em uma política sobre configuração e uso de um endpoint?

- Tipo de informação, nível de classificação e registro dos endpoints;
- Requisitos de proteção física;
- Restrição de instalação de software de controle remoto pelo admin;
- Requisitos para instalação de softwares, as versões e atualização automática ativa;
- Regras de conexão em redes públicas ou a obrigação do uso de um firewall;
- Controles de acesso;
- Proteção contra malware;
- Desativação, exclusão ou bloqueio remoto;



Política de Dispositivos

Endpoint do Usuário

O que deve constar em uma política sobre configuração e uso de um endpoint?



- Backups;
- Uso de web services (REST, XML, SOAP etc.) e aplicativos web;
- Análise do comportamento do usuário final;
- Uso de dispositivos removíveis, incluindo dispositivos de memória removíveis;
- A possibilidade de desabilitar portas físicas, por exemplo, portas USB;
- O uso do particionamento, para separar com segurança as informações dos softwares.

Responsabilidades dos Usuários com o BYOD e Conexões sem Fio

Além da conscientização no uso dos endpoints, os usuários devem:



Encerrar sessões ativas e serviços quando não forem mais necessários;



Proteger os endpoints contra o uso não autorizado com controles físicos e lógicos;



Usar dispositivos com cuidado em locais públicos, escritórios abertos etc;



Proteger contra roubo em carros, metrô, quartos de hotel, conferência e reunião;



Incluir seguro e outros requisitos de segurança em casos de roubo ou perda;

Responsabilidades dos Usuários com o BYOD e Conexões sem Fio

Para o uso do BYOD, devem:

- Separar o uso pessoal e comercial, incluindo o uso de software;
- Acessar às informações comerciais somente após reconhecerem deveres;
- Evitar disputas sobre direitos de propriedade intelectual desenvolvidos em BYOD;
- Permitir o acesso durante uma verificação de segurança ou uma investigação;
- Responsabilizar-se pelo licenciamento de software;



E quanto às conexões sem fio, a organização deve estabelecer procedimentos para:



Configuração, por exemplo, desabilitando protocolos vulneráveis;



Usar conexões sem fio ou com fio com largura de banda apropriada para, por exemplo, backups ou atualizações de software.

Controle: Instalação de Software em Sistemas Operacionais



Objetivo:

Garantir a integridade dos sistemas operacionais e evitar a exploração de vulnerabilidades técnicas.

Como evitar a exploração de vulnerabilidades em sistemas operacionais?



- Atualizações apenas por administradores treinados e com autorização;
- Garantir apenas código executável aprovado e não códigos de desenvolvimento ou compiladores;
- Instalação e atualização somente após testes extensivos e bem-sucedidos;
- Atualizar todas as bibliotecas de fontes de programas correspondentes;
- Usar um sistema de controle e documentação das configurações do sistema;

- Definir uma estratégia de reversão antes que as mudanças sejam implementadas;
- Manter um registro de auditoria de todas as atualizações;
- Arquivar versões antigas juntamente com todas as informações como medida de contingência.

Controle: Direitos de Acesso Privilegiado

Objetivo:

Garantir que apenas usuários autorizados, componentes de software e serviços sejam fornecidos com direitos de acesso privilegiado.



- Este tópico segue o que foi definido na Política de Controle de Acesso;
- A alocação de direitos de acesso privilegiado é controlada por meio de um processo de autorização formal.



Controle: Direitos de Acesso Privilegiado



O que são Direitos de Acesso Privilegiado?

- Direitos de acesso privilegiado são fornecidos a uma identidade, uma função ou um processo;
- São atividades que usuários ou processos típicos não podem realizar;
- Funções de administrador do sistema geralmente exigem direitos de acesso privilegiado;
- Exemplo, como sistemas de gerenciamento de banco de dados e aplicativos;
- Cuidado com o uso inapropriado de privilégios de administrador que pode anular os controles do sistema ou do aplicativo, pois contribui para falhas ou violações.

Considerações sobre os Direitos de Acesso Privilegiado

Considerações

- Alocar direitos de acesso privilegiado aos usuários conforme necessário;
- Alocar apenas a indivíduos com a necessária competência para realizar atividades;
- Manter um processo de autorização, ou seja, quem pode aprovar ou reprovar;
- Definir requisitos para caducidade dos direitos de acesso privilegiado;
- Garantir que os usuários estejam cientes quando estiverem no modo de acesso privilegiado;
- Requisitos de autenticação podem ser superiores aos acesso normais;
- Revisar os direitos privilegiados regularmente, e após qualquer mudança;
- Estabelecer regras específicas para evitar o uso de IDs genéricas como "root";



Considerações sobre os **Direitos de Acesso Privilegiado**

Considerações

- Conceder acesso temporário apenas na janela necessária para atividade aprovada;
- Registrar todos os acessos privilegiados aos sistemas para fins de auditoria;
- Não compartilhar ou vincular identidades a várias pessoas;
- As identidades podem ser agrupadas em um grupo para simplificar a gestão;
- Usar para realizar tarefas específicas e não para tarefas do dia-a-dia.



Controle: Restrição de Acesso à Informação



Objetivo:

Garantir apenas o acesso autorizado e impedir o acesso não autorizado a informações de sistemas, aplicativos e serviços.

O que é necessário para restringir o acesso a sistemas, aplicativos e serviços?



- Evitar o acesso a informações confidenciais por desconhecidos ou anônimos;
- Controlar quais dados podem ser acessados por um determinado usuário;
- Controlar tipo de acesso como leitura, gravação, exclusão e execução;
- Controles de acesso físico ou lógico para isolar itens sensíveis;

Controle: Restrição de Acesso à Informação

O que é necessário para restringir o acesso a sistemas, aplicativos e serviços?

- Considere usar técnicas e processos de gerenciamento de acesso dinâmico se:
 - ✓ Deve granular sobre quem, como e por quanto tempo pode acessar;
 - ✓ Compartilha tais informações com pessoas de fora da organização;
 - ✓ Deseja gerenciar dinamicamente, em tempo real, o uso e a distribuição;
 - ✓ Deseja proteger tais informações contra alterações, cópias e distribuição não autorizadas (incluindo impressão);
 - ✓ Deseja monitorar o uso das informações;
 - ✓ Deseja registrar alterações caso uma investigação futura seja requerida.



Brewer-Nash

- O modelo Brewer-Nash foi construído para fornecer controles de acesso que podem mudar dinamicamente;
- Conhecido como modelo Muralha da China ou “Muro Ético”;
- Modelo que atenua conflitos de interesses, pois:
 - ✓ Nenhuma informação pode fluir entre os sujeitos e objetos;
 - ✓ De forma que crie um conflito de interesses.
- O controle de acesso é baseado em risco;
- Projetado em torno de uma suposição de que os riscos mudam ao longo do tempo;
- Respondem a mudanças dinâmicas em tempo real e não são estáticas.



Brewer-Nash

Por exemplo:

- Um escritório de advocacia representando clientes concorrentes;
- Um analista financeiro operando ações com empresas adversárias;
- Um mestre cervejeiro criando uma receita para duas cervejarias distintas;
- Uma consultoria estratégica atuando em um mercado com empresas do mesmo ramo.



Técnicas de Gerenciamento de Acesso Dinâmico

Essa técnica deve proteger as informações ao longo de seu ciclo de vida (ou seja, criação, processamento, armazenamento, transmissão e descarte), incluindo:

- Permissões de acesso com base na identidade, dispositivo, localização ou aplicativo;
- Esquema de classificação;
- Estabelecimento de processos de monitoramento, relatórios e suporte técnico;
- Autenticação, credenciais apropriadas ou certificado para acessar as informações;
- Acesso a um período de tempo especificado;

Técnicas de Gerenciamento de Acesso Dinâmico

Essa técnica deve proteger as informações ao longo de seu ciclo de vida (ou seja, criação, processamento, armazenamento, transmissão e descarte), incluindo:

- Criptografia para proteger as informações;
- Permissões de impressão das informações;
- Quem acessa a informação e como a informação é utilizada;
- Alertas caso sejam detectadas tentativas de uso indevido das informações.

Considerações



- Não substituem o gerenciamento de acesso clássico, por exemplo, ACLs;
- Útil para resposta a incidentes, pois as permissões podem ser modificadas ou revogadas a qualquer momento.

Controle: Acesso ao Código Fonte



Objetivo:

Evitar a introdução de funcionalidades não autorizadas, evitar alterações não intencionais ou maliciosas e manter a confidencialidade da propriedade intelectual valiosa.

O que devemos proteger além do código-fonte?

■ Itens associados:

- ✓ Projetos;
- ✓ Especificações;
- ✓ Dados em produção, desenvolvimento, teste, homologação etc.;
- ✓ Configurações;
- ✓ Versionamento;
- ✓ Biblioteca;
- ✓ Planos de teste, integração etc.



Controle: Acesso ao Código Fonte

O que devemos proteger além do código-fonte?

■ Ferramentas de desenvolvimento:

- ✓ Compiladores;
- ✓ Construtores;
- ✓ Ferramentas de integração (DevOps);
- ✓ Plataformas de teste;
- ✓ Ambientes.



Evitando o Acesso ao Código-Fonte

Medidas para controle de armazenamento ao código-fonte:

- Controle de acesso de leitura a um repositório de código centralizado;
- Usar um sistema de gerenciamento de código-fonte;
- O acesso de leitura e gravação com base na função e em pessoas com privilégios;
- Aplicar controles se o código-fonte for aberto ou de terceiros;
- Diretrizes para controlar o acesso às bibliotecas de origem do programa;
- Conceder acesso de leitura e gravação com base nas necessidades do negócio;
- Concessão de acesso com base nos procedimentos de controle de mudanças;
- Não conceder aos desenvolvedores acesso direto ao repositório de código-fonte;
- Manter e gerenciar uma lista de programas em um ambiente seguro;
- Manter um registro de auditoria de todos os acessos e de todas as alterações;
- Controles adicionais para garantir integridade, como assinatura digital.



Controle: Autenticação Segura



Objetivo:

Garantir que um usuário ou uma entidade seja autenticado com segurança quando o acesso a sistemas, aplicativos e serviços é concedido.

Como comprovar a identidade real de um usuário, software, mensagem ou outras entidades?

- A força da autenticação deve ser adequada à classificação das informações;
- O método da autenticação forte pode ser através de certificados digitais, smart cards, tokens ou meios biométricos;
- Autenticações devem ser acompanhadas por autenticação multifator:



O que você sabe;



O que você tem;



O que você é.

- A autenticação biométrica deve ser invalidada se for comprometida devido a umidade ou envelhecimento;
- Para problemas de biometria, deve ser acompanhada de pelo menos uma técnica de autenticação alternativa.

Procedimentos e Tecnologias para Logins

O procedimento para efetuar login em um sistema ou aplicativo deve ser projetado para minimizar o risco de acesso não autorizado.

Os procedimentos e tecnologias de login devem ser implementados considerando o seguinte:

- Não exibir informações confidenciais até que o login tenha sido completado;
- Exibir um aviso que o sistema só deve ser acessado por usuários autorizados;
- Não fornecer mensagens de ajuda durante o procedimento de login;
- Validar as informações após o preenchimento de todos os dados de entrada;
- Proteger contra força bruta em nomes de usuário e senhas, como CAPTCHA;

Procedimentos e Tecnologias para Logins

Os procedimentos e tecnologias de login devem ser implementados considerando o seguinte:

- Exigir redefinição de senha após um número de tentativas com falha;
- Bloquear o usuário após um número máximo de erros;
- Registro de tentativas malsucedidas e bem-sucedidas com alerta ao admin;
- Exibir informações sobre a data do último login bem e malsucedido;
- Não exibir uma senha em texto ao ser digitada;
- Não transmitir senhas sem criptografia em uma rede para evitar um sniffer;
- Encerrar sessões inativas após um período definido de inatividade;
- Restringir tempo de duração da conexão.

Programas Utilitários

Qual a finalidade?

- Ajuda na execução do sistema operacional e na manutenção geral do sistema;
- Executa uma tarefa específica com funções úteis, como formatação, compactação, digitalização, exploração etc.

Tarefas comuns realizadas por Programas Utilitários



Desfragmentação de disco;



Limpeza de disco;



Gerenciamento de arquivos;



Backup;



Depuradores;

Programas Utilitários

Tarefas comuns realizadas por Programas Utilitários



Ferramenta de Diagnóstico;



Monitoramento de rede;



Compressão;



Gerenciamento de Disco;



Antivírus;



Firewall;



A maioria dos endpoints tem um ou mais programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações!

Controle: Uso de Programas Utilitários Privilegiados

Objetivo



Garantir que o uso de programas utilitários não prejudique o sistema e os controles de aplicativos para a segurança da informação.

Como evitar que os utilitários prejudiquem os sistemas e substituam os controles?

- Limitar o uso desses programas somente a usuários autorizados;
- Usar de procedimentos de identificação, autenticação e autorização;
- Definição e documentação dos níveis de autorização;
- Não disponibilizar utilitários para usuários que tenham acesso aos sistemas;
- Remover ou desabilitar todos os programas utilitários desnecessários;
- Segregação lógica dos programas utilitários do software;

- Se possível, segregar comunicações de rede para esses programas do tráfego de aplicativos;
- Limitar a disponibilidade dos utilitários durante uma mudança autorizada;
- Registrar todos os usos de programas utilitários.

OBRIGADO



**ISF – CONTROLE DE ACESSO A
SISTEMAS E ENDPOINT**
