58BR

CIBERSEGURANÇA.

Conversando sobre "Cibersegurança"

Primeiramente é importante definir com clareza o que é cibersegurança. Para isto vamos começar desde o início.

Qualquer equipamento eletrônico que tenha um sistema operacional recebe comando do Software para promover ações no Hardware. A partir daí entendemos que "*receber comandos*" é a parte vulnerável deste processo. Esta brecha não é proposital ela é natural do processo.

O sistema operacional permite a instalação de outros programas com funcionalidades específicas : editor de texto, planilha eletrônica, agenda entre outros. Permite também aplicações como : ERP, PDV, frente de caixa, folha de pagamento, controle de comandas e muito mais. Todos estes também enviam "*comandos* que devem ser obedecidos.

Na primeira camada de segurança existe o **antivírus**, denominado hoje ENDPOINT (traduzindo: *o que está na "Ponta Final"*), abreviando EDR que quer dizer Detecção e Resposta na Ponta final (**Endpoint Detection and Response)**.

Existem vários no mercado, muitos de excelente qualidade e fáceis de instalar e usar. Mas, lembramos que ele é "instalado" em um equipamento com um sistema operacional presente, superior em hierarquia operacional. Sendo assim alguns cuidados são necessários.

Há também o risco de um usuário que saiba "desativar", "suspender" ou até remover o antivírus. Atualmente a maioria dos antivírus coloca uma senha para estes recursos evitando que um usuário simplesmente decida comprometer o computador.

Na próxima camada que é a Rede, e-mail, Nuvem e o próprio Endpoint vem o XDR **(Extended Detection and Response)** que quer dizer camada e**X**tendida de detecção e resposta. Com maior abrangência sobre a "transferência dos dados" de um ponto a outro, monitora os "*comandos implícitos*" que podem ocasionar todo o tipo de prejuízo. Esta é apenas

uma das muitas atividades feitas pelo XDR, pois estamos falando agora de "caminhos" e "endereços" externos ao seu ambiente de trabalho.

Esta camada é que basicamente alimenta a próxima camada, o MDR que quer dizer camada gerenciada de detecção e resposta **(Managed Detection and Response).** Esta camada de segurança é externa ao seu ambiente operacional e se alimenta dos dados e alertas gerados nas camadas anteriores. Sua principal função é identificar "*comportamentos*" não habituais e interromper.

Há uma certa resistência entre os gestores de TI de acreditar que a sua equipe consegue controlar esta atividade. Capacidade técnica não falta, mas desenvolver as suas atividades diárias de TI : backup, restauração, gerenciamento dos bancos de dados, manter a conectividade, manter os sistemas operantes e íntegros, suporte, helpdesk e infraestrutura pode "distrair" a sua equipe bem no momento de uma invasão.

Sendo assim, um gestor deve considerar terceirizar esta função para alguma empresa que trabalhe 24x7 (normalmente as equipes de MDR estão em locais diferentes do mundo cobrindo as 24 horas do dia).

Na primeira camada o usuário pode muito bem resolver alguns problemas identificados pelo EDR. Existe também suporte técnico para este fim.

Na segunda camada, que requer mais conhecimento técnico, muitos problemas também podem ser resolvidos pela sua equipe de TI (interna ou terceirizada).

Já na terceira camada de proteção o agente informa ao cliente que algo "fora do comum" está em curso e para isto tem ferramentas que segregam o processo a uma área externa (denominada SANDBOX traduzindo caixa de areia) onde procede os testes para identificar qualquer comando ou ação maliciosa prejudicial ao seu ambiente. O agente avisa, enquanto simula os resultados e pode interromper caso seja risco.

Cibersegurança então é reunir todas estas camadas para que juntas aumentemos a segurança do seu ambiente, dos seus processos e dos seus dados.

Existem muitos pontos adicionais em cada camada, mas o texto ficaria muito grande e cansativo para ler e formar o conceito de cibersegurança.

Um usuário mal treinado (na melhor das situações) ou mal intencionado (na pior situação) pode comprometer o seu computador, o sistema ou a rede com um simples anexo ou um Pen drive.

O uso de cabos USB para conectar dispositivos pode ser outra fonte de Risco. E existem muitos outros Riscos que passam desapercebidos a maioria das pessoas.

É nosso objetivo informar para despertar a atenção de forma que você possa procurar uma empresa que possa esclarecer mais sobre os Riscos ao seu ambiente e oferecer soluções mais potentes ao combate aos cibercriminosos.

Fazemos um aparte aqui, assim como existe aquele que combate as invasões estudando e aprendendo mais sobre as brechas, existe também aquele que estuda e aprende para se aproveitar delas para obter lucros indevidos (Ransomware, por exemplo).

Muito comum o empresário pensar : "sou muito pequeno" quem vai querer mexer na minha empresa ?

Para estes, lembramos que na outra ponta desta situação está alguém disposto a obter lucro e não vê a sua empresa, vê somente um IP (endereço de rede da internet). Por este motivo é que alertamos para a consciência de que você pode estar mais exposto do que imagina.

Ficamos a disposição para uma conversa de avaliação do ambiente apontando eventuais melhorias apropriadas a sua capacidade financeira. Existem soluções de vários produtos, fabricantes e abrangência.

Hoje elaboramos uma pesquisa pelo Google Forms para "sentir" como estão sobre "PROTEÇÃO e SEGURANÇA", se desejar conhecer os resultados clique no link : https://forms.gle/LTnVruT1oEd7oGoa9

São Paulo, 14 de novembro de 2025.

Sergio Rodrigues Teixeira

Técnico Responsável