

NOVO MOMENTO



Governança é a chave para prevenir ransomware nas empresas

O volume de ataques cibernéticos só vem crescendo mundialmente, o que tem tirado o sono dos especialistas em segurança e proteção de dados de empresas.

Segundo previsões do Gartner Group, 60% das grandes organizações devem usar uma ou mais técnicas de computação que melhorem a segurança das informações até 2025.

Empresas que adotarem, até 2024, malhas de segurança cibernética para integrar ferramentas de segurança vão reduzir o impacto financeiro de incidentes individuais em cerca de 90%. De acordo com a International Data Corporation (IDC), 80% das empresas precisarão reestruturar seus processos de governança até 2025.

Estabelecer processos é o primeiro passo para criar uma política de prevenção de ataques e incidentes.

Organizar as atividades e responsabilidades da empresa é a medida de prevenção mais assertiva, e passa pela conscientização de que as principais falhas que estão nos processos podem, sim, ser mitigadas. Empresas de qualquer tamanho podem e devem adotar procedimentos e controles pra ter uma estratégia de atuação e prevenção contra invasões, começando pelo desenho dos processos de Governança e Compliance.

Um programa de prevenção de ransomware – ameaça de maior ocorrência atualmente - consiste em seguir cinco etapas, que correspondem ao modelo baseado nos ciclos de vida do National Institute of Standards Technology (NIST): Identificar, Proteger, Detectar, Responder e Recuperar. São mais de 500 controles unificados para que, na prática, possamos trabalhar com um total de 30 controles a serem implementados durante os ciclos de vida.



Sistemas de gestão de Segurança, Continuidade, Riscos e Proteção de Dados bem efetivos trarão aos softwares algum grau de segurança, como DLP's, SIEM, Antivirus, Firewall's, entre outros. Mas o principal está na organização das atividades e responsabilidades das empresas, ações que, embora sejam simples, são cruciais para manter as empresas mais protegidas das vulnerabilidades.

Softwares de atualizações e patches de segurança – em 2021 foram relatadas 21.957 CVEs (vulnerabilidades e exposições comuns), um aumento de 19,6% em relação a 2020, segundo o relatório Threat Landscape Retrospective 2021. Atentar-se aos anúncios de atualização, que geralmente são divulgados com antecedência, e utilizar soluções de gerenciamento de patches eficientes são alternativas para manter os softwares críticos para a empresa rodando.

Logins e senhas – senhas fracas permitem que criminosos entrem nas redes com logins legítimos, dificultando a detecção de atividades maliciosas. Adotar softwares de gerenciamento de senhas ajuda nessa missão, pois os algoritmos criam senhas aleatórias, naturalmente mais fortes, que ficam conectadas a todas as plataformas

utilizadas na empresa, ou seja, uma camada a mais de proteção.

Acessos remotos - A VPN (Virtual Private Network) é um recurso de cibersegurança, que permite que o tráfego de dados na internet seja feito de forma privada, funcionando como um firewall. VPNs de SSL não corrigidas são brechas para que invasores façam espionagem cibernética, capturem informações confidenciais e criptografem redes.

A VPN não funciona como antivírus, ela apenas protege o IP e criptografa o histórico de navegação na internet. Para ajudar a proteger o comprometimento das redes, as organizações podem aplicar a autenticação multifator em toda a rede.

Vale lembrar que ataques de phishing - em que os criminosos cibernéticos enviam e-mails contendo um anexo malicioso ou direcionam as vítimas para um site comprometido que entrega ransomware - e ataques contra serviços de RDP - onde os criminosos forçam brutalmente nomes de usuário e senhas fracas ou padrão - continuam sendo portas de entrada populares para ransomware, a ameaça que mais tem causado estragos atualmente, tanto para empresas quanto para usuários.

Fazer o básico bem feito e construir um ecossistema de governança e compliance condizente com a realidade da empresa é o que tornará os sistemas eficazes.

A pandemia mudou a forma de monitoramento e proteção de redes nas organizações e, com a migração de dados para plataformas de nuvem e a dependência de provedores de serviços gerenciados, principalmente nas empresas que não têm equipe de TI própria, veio a necessidade de focar em desafios de segurança antigos para dirimir riscos.

(Fonte: Sylvio Sobreira é CEO da SVX Corporate - www.svxconsultoria.com.br.)

Negócios em Pauta

Foto: automaistv.com/reprodução



Tecnologia, máquinas, borracha e pneus

As duas maiores feiras de tecnologia, máquinas e artefatos de borracha e da indústria de pneus da América Latina serão realizadas entre os dias 22 a 24 de junho, no Expo Center Norte, após um hiato de quatro anos. Quase 200 expositores e milhares de compradores e profissionais do setor, nacionais e internacionais estarão presentes. A Expobor (Feira Internacional de Tecnologia, Máquinas e Artefatos de Borracha) e a Pneushow (Feira Internacional da Indústria de Pneus) são, desde 1996, as principais feiras de negócios do setor. Abrangem produtos, máquinas, soluções e inovações para a transformação e produção de artefatos de borracha nos mais variados segmentos industriais, como automobilístico, eletrônica, petróleo e gás, siderurgia, calçados, entre outros (<https://expobor.com.br/credenciamento/>).

▶▶ Leia a coluna completa na página 5

News@TI

Imagem: AI/SERPRO



Startups podem se inscrever no Serpro Booster a partir desta quinta

@O Serpro divulga, nesta quinta-feira, dia 19, edital para inscrição no Programa Serpro Booster, que oferece créditos de consumo de produtos da empresa para startups de todo o país. O lançamento será transmitido pelo canal do Serpro no Youtube a partir das 15h. O programa foi pensado para promover um ambiente de inovação e colaboração entre o governo e a sociedade, através da interação com os ecossistemas de inovação e empreendedorismo e empresas startups. Para participar, basta acessar a página do Serpro Booster e preencher formulário eletrônico de inscrição, que é gratuita (<https://booster.serproventures.estaleiro.serpro.gov.br/register>). ▶▶ Leia a coluna completa na página 6

Estratégia de conteúdo: tudo que você precisa saber

Com as mudanças da internet e com a drástica queda no alcance de publicações nas redes sociais, construir uma estratégia de conteúdo não tem sido uma tarefa fácil para as marcas atualmente. ▶▶

Como o atendimento pode construir (ou não) a percepção de uma marca

Em um mundo cada vez mais conectado, competitivo e com consumidores exigentes, as empresas precisam se diferenciar para fidelizar e conquistar seus clientes. ▶▶

Ataques cibernéticos: empresas estão no modo “apagar incêndio”

Ataques cibernéticos que comprometem empresas e órgãos públicos cresceram nos últimos anos, especialmente durante a pandemia. ▶▶

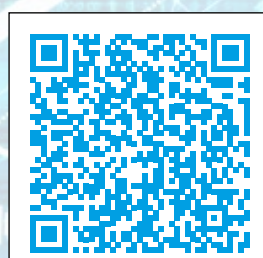
Crie a sua Persona e humanize o atendimento ao cliente

A melhor forma de conquistar os seus clientes é através do conteúdo humanizado e exclusivo e você pode contar com a Persona para te ajudar com isso! Quer se tornar uma empresa customer centric e atender os seus clientes com a exclusividade que eles buscam? Então chegou a hora de você criar a sua Persona. ▶▶

Para informações sobre o

MERCADO FINANCEIRO

faça a leitura do QR Code com seu celular



Empreendedorismo

Não existe Líder sem agenda de liderança

Costábile Matarazzo

▶▶ Leia na página 4

