www.netjen.com.br
ISSN 2595-8410

Sexta-feira,
27 de novembro de 2026

Ano XXII - Nº 5.717

Empresas & Negócios

Leilão de relógios

Relógios de marcas como Rolex, Omega, Cartier, TAG Heuer, Longines e Tissot estarão entre os destaques da 3ª edição do Master Leilão de Relógios 2026, promovido pelo Bid Leilão no dia 7 de dezembro, às 19h, em formato online. O catálogo apresenta modelos de diferentes épocas e estilos, incluindo exemplares automáticos, cronógrafos, relógios vintage e peças de ouro (https://www.bid-leilao.com.br).

SergeyNivens_CANVA



NECESSIDADES DE CONSUMO

CINCO SINAIS DE QUE AS PEQUENAS COMPRAS ESTÃO MUDANDO O VAREJO

Leia na página 8

Sistemas legados, IoT e IA

O cenário perfeito por trás da nova onda de sabotagem digital

Sistemas legados, IoT e IA: o cenário perfeito por trás da nova onda de sabotagem digital

Nas últimas semanas, o mundo foi impactado por ataques cibernéticos de grande repercussão e prejuízos financeiros inéditos. O roubo histórico de US$ 6,34 bilhões na corretora de criptomoedas Binance, executado em apenas 20 minutos após a infecção do computador de um engenheiro, as invasões a sistemas de refrigeração de centenas de supermercados na Europa e o ataque a bancos de sangue na França chamam a atenção da sociedade e de especialistas para a gravidade do cenário atual. No Brasil, a realidade não é diferente; muito pelo contrário, a onda de ofensivas digitais segue causando estragos. O vazamento de credenciais que comprometeu o sistema público de videomonitoramento SmartSampa, o bloqueio preventivo de ativos no Mercado Bitcoin e a recente invasão que tirou do ar os sistemas do Porto de Santos (SP) expõem a fragilidade das infraestruturas críticas e colocam em xeque a maturidade de empresas nacionais e multinacionais em segurança da informação.

O que estamos testemunhando hoje vai muito além do cibercrime tradicional focado apenas em extorsão financeira. Estamos diante de uma escalada de ações com objetivo claro de sabotagem e terrorismo digital, cujo objetivo é paralisar cadeias de suprimento, gerar pânico social e causar danos físicos reais. Ao elevar remotamente a temperatura de câmaras frigoríficas no varejo europeu ou ameaçar estoques de sangue em hospitais, os atacantes demonstram que a fronteira entre o ambiente digital e o mundo físico desapareceu.

Esse cenário, embora alarmante, não é uma surpresa para quem acompanha a evolução dos riscos tecnológicos. Institutos de pesquisa já alertavam há anos que a convergência desordenada entre Tecnologia da Informação (TI) e Tecnologia Operacional (TO) cobraria um preço alto. E a conta parece que chegou. Em 2021, a consultoria Gartner, por exemplo, já havia projetado o crescimento acelerado de ataques contra Sistemas Ciberfísicos (CPS) alertando que criminosos transformariam ambientes industriais e de TO em armas capazes de causar danos físicos reais. Mais recentemente, o próprio Gartner reforçou essa projeção ao apontar que, até 2028, falhas e invasões envolvendo configurações inadequadas em softwares de sistemas

Divulgação



Natália Santos

> O que estamos testemunhando hoje vai muito além do cibercrime tradicional focado apenas em extorsão financeira.

críticos e IA poderão provocar o desligamento de infraestruturas críticas em países da Europa.

Vulnerabilidade de dispositivos IoT

A causa raiz por trás de episódios como o dos supermercados europeus reside em um problema crônico da indústria e do varejo: a vulnerabilidade de dispositivos IoT (Internet das Coisas) conectados à rede sem a devida proteção. Muitas dessas operações dependem de equipamentos físicos que rodam sistemas legados — softwares antigos que foram projetados para durar décadas, mas que já não recebem atualizações de segurança dos fabricantes. Quando uma empresa conecta esse parque tecnológico obsoleto à internet em nome da automação, sem segmentação de rede ou monitoramento contínuo, cria-se uma porta aberta para invasores.

Com a chegada e a democratização do uso da Inteligência Artificial o cenário passou a funcionar como um catalisador dessa crise. Se antes descobrir uma falha em um controlador industrial exigia semanas de trabalho manual, hoje grupos cibercriminosos utilizam modelos de IA para mapear automaticamente superfícies de ataque, identificar dispositivos expostos e explorar vulnerabilidades em escala global e velocidade sem precedentes. Não à toa, o próprio Gartner já projetava que o volume de vulnerabilidades de software conhecidas saltaria de 277 mil em 2025 para mais de 1 milhão até 2030, tornando os modelos tradicionais de defesa reativa completamente insuficientes.

Então, por mais sofisticada que seja a tecnologia utilizada no ataque, a porta de entrada quase sempre continua sendo a mesma: o fator humano. O caso da Binance ilustra perfeitamente essa dinâmica — bilhões de dólares foram desviados não por uma quebra matemática na criptografia da corretora, mas por um golpe de engenharia social direcionado a um colaborador. Em seu relatório sobre as principais tendências de cibersegurança, o Gartner também reforça que os programas tradicionais de conscientização falham diante de golpes potencializados por IA generativa, exigindo abordagens comportamentais adaptativas.

É exatamente nesse ponto que reside a virada de chave para as organizações. Não basta mais investir milhões em firewalls e ferramentas de perímetro se os colaboradores continuam agindo de maneira indevida e se colocando vulneráveis à manipulação de criminosos ou se negligenciam políticas básicas de segurança da informação. Hoje as organizações precisam acompanhar diariamente como a gestão contínua do risco humano transforma o comportamento corporativo. Quando medimos o nível de exposição de cada área e capacitamos as pessoas de forma personalizada e constante, reduzimos drasticamente a propensão ao erro e ao clique malicioso.

Os incidentes recentes no Brasil e no exterior deixam uma lição inadiável para conselhos de administração e lideranças executivas: a resiliência cibernética moderna exige duas frentes trabalhando em total sintonia: a modernização e o isolamento rigoroso de ativos físicos e sistemas legados, aliados a uma cultura viva de monitoramento do comportamento humano. Ignorar qualquer um desses pilares significa assumir o risco de TI, ou seja, colocar em risco a continuidade do próprio negócio e a segurança da sociedade.

(Fonte: Natália Santos é Gerente de Marketing e Canais da Beephish).

Negócios em Pauta

Divulgação



Influência digital entra no planejamento empresarial de 2027

Como transformar presença digital em oportunidades de negócio será o tema do Tittanium Day Missão Influence, marcado para 1º de dezembro, no Jota Lab, em Alphaville, Barueri, na Grande São Paulo. Voltado aos sócios do Tittanium Club, o encontro discutirá posicionamento, produção de conteúdo e construção de autoridade como parte do planejamento empresarial para 2027. À frente da iniciativa está Fernanda Tochetto, psicóloga e fundadora do Tittanium Club, comunidade voltada ao desenvolvimento de empresários. A proposta é orientar os participantes a definir como desejam ser reconhecidos pelo mercado e quais ações precisam adotar para aproximar essa percepção dos objetivos de suas empresas (https://www.fernandatochetto.com.br/).

Leia a coluna completa na página 3

News@TI

Rafael Cautella



Dabi Business Park recebe V Feira de Tecnologia da Barão de Mauá

@Como um técnico pode registrar um atendimento no campo mesmo quando está sem internet? O que ajuda uma pessoa idosa a usar o celular com mais autonomia e a reconhecer tentativas de golpe? E como apresentar os dados da rede pública de ensino de Ribeirão Preto de modo que pais e estudantes consigam consultá-los? Alunos de Ciência da Computação da Barão de Mauá partiram dessas perguntas para propor soluções para desafios reais de empresas e entidades. Na V Feira de Tecnologia da Barão de Mauá, que será realizada em 2 de dezembro no Dabi Business Park, o público poderá conhecer esses e outros projetos desenvolvidos no semestre na disciplina Fábrica de Software. Os trabalhos partem de dificuldades do dia a dia de empresas, instituições e da comunidade. Um pequeno comerciante precisa de um jeito simples de controlar vendas e estoque. Uma clínica de psicologia precisa reunir registros de atendimento e restringir o acesso a informações confidenciais.

Leia a coluna completa na página 2

A próxima vantagem competitiva no crédito não está no saldo bancário

Imagine dois brasileiros com o mesmo extrato bancário nos últimos seis meses. O primeiro acabou de perder o emprego com carteira assinada e está vivendo da rescisão.

IA pode acelerar o Brasil, mas educação e eficiência vão definir o ritmo

Combinação de vantagens que poucos países conseguem reunir: um mercado consumidor expressivo, recursos naturais abundantes, capacidade empreendedora e profissionais reconhecidos pela criatividade.

Setor de cuidados impulsiona o empreendedorismo feminino

Aumento da expectativa de vida impulsiona a busca por serviços especializados e abre espaço para novos modelos de negócio.

Marketing de influência exige estratégia para marcas não ficarem em segundo plano

Escolha do criador, integração do produto ao conteúdo e identidade visual ajudam empresas a transformar exposição em reconhecimento e fortalecer a presença nas campanhas de fim de ano.

Para informações sobre o
MERCADO FINANCEIRO
faça a leitura do
QR Code com seu celular

Política

Boatos de fim do mundo

Heródoto Barbeiro



Leia na página 2

Economia da Criatividade

Internacionalização como Estratégia de Marca: Como Comunicar uma Educação sem Fronteiras?

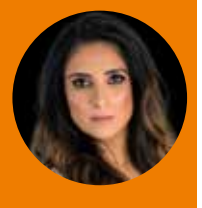


Carol Olival

Leia na página 6

Negócios & Carreira!

Ninguém vira líder sem aprender primeiro



Fabiana Monteiro

Leia na página 7