Política de cibersegurança protege empresas de ataques como ransomware

OBrasil está entre os dez países que mais registram ataques do tipo ransomware, que se caracterizam pelo sequestro e criptografia de dados, com o grupo criminoso exigindo o pagamento de um resgate para tornar essas informações novamente acessíveis para a empresa que foi vítima do cibercrime

O que torna esse cenário mais preocupante é que apenas 26% das empresas brasileiras estão maduras o suficiente para resistir aos ciberataques, de acordo com estudo da Cisco. Ainda segundo esse levantamento, quase sete em cada dez empresas esperam que um incidente de segurança cibernética interrompa suas atividades no intervalo de 12 a 24 meses.

O Fórum Econômico Mundial, no relatório "The Global Risks Report 2023", apontou a propagação dos crimes cibernéticos ao lado do crescimento da insegurança cibernética como o oitavo maior risco global tanto no curto prazo como no longo. Para curto prazo, o estudo considerou até dois anos e, para longo, até dez anos. Esse risco inclui incidentes de segurança da informação, como vazamento de dados, que resultam em ameaça à privacidade dos cidadãos.

Neste ano, os respondentes – mais de 1,2 mil especialistas de universidades, negócios, governos, comunidade internacional e sociedade civil – disseram que os ataques cibernéticos à infraestrutura crítica produzirão os impactos mais severos ou significativos em escala global. Nesse contexto, as empresas devem contar com uma política bem estruturada de cibersegurança em seus programas de conformidade em proteção de dados.

peshkov_CANVA

Apenas 26% das empresas brasileiras estão maduras o suficiente para resistir aos ciberataques.

Essas diretrizes são formadas por cinco funções ou capacidades essenciais: identificação de riscos; proteção de ativos de informação; detecção de riscos em evolução; resposta a riscos que se materializam; e recuperação de danos provocados por um risco. Boa parte do compliance com a LGPD (Lei Geral de Proteção de Dados) e outras legislações do mundo, como o GDPR (regulamento de proteção de dados vigente na União Europeia), está associado à capacidade de proteger as informações corporativas, incluindo dados pessoais de colaboradores e clientes, de ameaças internas e externas.

"Toda organização deve ter duas preocupações básicas: evitar o tratamento indevido ou inadequado dos dados pessoais armazenados em suas bases e ser capaz de garantir a segurança dessas informações", diz Marcos Sêmola, sócio da EY para consultoria em cibersegurança.

No primeiro caso, a própria empresa, que é considerada um agente de tratamento pela LGPD, pode agir em desconformidade com a legislação caso perca, por exemplo, os dados do titular ou não atenda a uma solicitação dele, como a de retificação dos dados, exclusão ou fornecimento dos dados aos titulares. Já no segundo caso, a empresa pode falhar na garantia da confidencialidade, integridade ou disponibilidade dos dados, ainda que seja vítima de um incidente de segurança da informação.

- **Erro humano é a porta de entrada das ameaças -** O Fórum Econômico Mundial constatou que 95% dos problemas de segurança cibernética são causados por erro humano. "É aquele exemplo clássico do colaborador que recebe um e-mail com link de phishing, clicando nele e contaminando toda a rede corporativa com vírus. Essa costuma ser a porta de entrada do ransomware", diz Sêmola.

"Esse evento produz diversos problemas em cascata, como reputacionais, financeiros e operacionais, já que a empresa fica nas mãos dos criminosos e completamente parada por um tempo que ninguém consegue prever", finaliza. Para amenizar esse risco de erro humano, a recomendação é que as organizações promovam periodicamente sessões de treinamento dos seus colaboradores, especialmente dos novos contratados. Fonte: Agência EY. Mais informações pelo e-mail (ey@fsb.com.br).

KPMG aponta quatro pontos sobre segurança cibernética no metaverso

A KPMG divulgou um levantamento que elenca quatro principais pontos referentes à segurança cibernética que devem ser levados em consideração pelos líderes durante o uso do metaverso. São eles: representação digital, interoperabilidade, risco de aquisição de conta e proteção de dados.

De acordo com a publicação, as oportunidades de crescimento continuarão a surgir à medida que as interações digitais se tornarem mais imersivas e contextuais, mas do ponto de vista da segurança cibernética, essas novidades não estão isentas de riscos.

"Nesse momento de disrupções, os líderes de segurança desempenham papel de destaque na intenção de qualquer empresa de utilizar o metaverso. São eles que, ao se engajarem ativamente em trazer inovações para os mercados, têm a incumbência de proteger tanto os clientes quanto os investimentos.

Assim, são fundamentais para estabelecer a confiança necessária ao sucesso dessas iniciativas", disse a sócia-diretora de inovação e transformação da KPMG no Brasil e co-fundadora da KPMG e Distrito Leap, Thammy Marcato.

As quatro considerações de risco que os líderes de segurança e os inovadores do metaverso precisam levar em conta, segundo a KPMG, são:

- **Representação digital -** A identidade é a base da segurança digital. É o elemento central para a construção da confiança. Essa certeza depende da solidez dos instrumentos e meios de verificação e asseguração de identidade.
- **Interoperabilidade** - Independentemente de quem esteja conectando vários metaversos (centralizados ou descentralizados), a possibilidade de trazer seu avatar, sua identidade digital e seus ativos, como token não fungíveis (NFTs) e criptomoedas, cria riscos importantes de segurança e fraude para o ecossistema mais amplo.
- **Risco de aquisição de conta** - À medida que a economia do metaverso floresce, as pessoas tendem a usar o espaço virtual para comprar ou vender seus produtos - e, assim, haverá muita movimentação de dinheiro.
- **Proteção de dados/uso indevido** - Tecnologias imersivas, como a realidade virtual e a realidade aumentada, oferecem a oportunidade de coletar muito mais informações do que os dispositivos móveis podem gerar. Se existem muitos dados circulando, é fundamental tomar medidas para protegê-los.

Por fim, o sócio-líder de segurança cibernética e privacidade da KPMG no Brasil e na América do Sul, Leandro Augusto, disse: "O metaverso evolui com rapidez e os líderes de segurança precisam permanecer vigilantes, trabalhando com as diversas partes envolvidas para construir um programa de segurança cibernética. Ao fazer isso, eles inspirarão confiança, criando as condições ideais para crescer, inovar e ter sucesso".

Publicidade legal em jornal é obrigação. Tá legal?

Os cuidados e as vantagens para quem busca investir em crédito privado

Gabriel Nascimento (*)

anyaberkut_CANVA

Avaliar o risco e o retorno dos ativos é muito importante para evitar surpresas no futuro.

Crédito privado é o nome dado a qualquer instrumento de renda fixa emitido por grandes empresas não financeiras para custear operações

Nos últimos anos, fintechs e fundos de crédito surgiram para desburocratizar e agilizar a demanda por novos tipos de investimentos. Essas empresas utilizam a estratégia de conectar investidores, que já buscam massivamente sair dos investimentos bancários tradicionais, às empresas que precisam de capital de giro. Avaliar o risco e o retorno dos ativos é muito importante para evitar surpresas no futuro.

Cada tipo de investimento envolve dinâmicas diferentes, mas hoje existem consultorias e profissionais especializados que podem orientar e calcular essa variável em cada aplicação.

O índice de Sharpe, por exemplo, é amplamente utilizado na avaliação de fundos de investimentos.

A metodologia pode ser a chave para o investidor, já que expressa a relação risco versus retorno e informa se o fundo oferece rentabilidade compatível com o "perigo" a que está exposto. Quanto maior o índice de Sharpe do fundo, desde que positivo, mais equilibrada e atraente é a relação entre o risco e o retorno.

As chances de um investimento dar errado é proporcional à possibilidade do tamanho do retorno. Por isso, um grande risco está muitas vezes ligado a um grande retorno. Por exemplo: quando se investe em uma startup, não há garantia de que a nova empresa irá prosperar. Porém, se crescer, os retornos investidos serão proporcionais. Já o risco de investir em uma empresa consolidada é muito menor, pois as chances de ir à falência são baixíssimas. Com isso, o retorno também é menor.

No mercado financeiro, o risco representa o potencial do investidor em arcar com prejuízos. No geral, as mudanças que ocorrem estão associadas a fatores econômicos, oscilações de mercado, política monetária, inflação e outros indicadores.

Em um cenário de rápidas transformações, as alternativas ficam cada vez mais acessíveis. Por isso, investir em crédito privado se torna mais atrativo. A primeira vantagem é a possibilidade de rentabilidade melhor do que mercados tradicionais de renda fixa, e volatilidade menor do que a grande maioria dos instrumentos de renda variável.

A diversificação é mais um ponto positivo e reduz o risco, especialmente em momentos de crise. O investidor pode trabalhar com fundos de crédito privado, distribuindo o dinheiro em diversas aplicações e, assim, reduzindo o risco. Uma carteira diversificada pode se beneficiar de ativos de crédito privado que costumam pagar remunerações mais altas.

O conhecimento das características de remuneração, dos riscos e das estratégias de mercado é fundamental para o brasileiro navegar em novas águas. Por fim, vale mencionar que alguns títulos de crédito privado apresentam isenção de Imposto de Renda, especialmente quando as debêntures são emitidas para financiar projetos que interfiram em infraestrutura e tragam benefícios para a população.

Há alguns anos, qualquer investimento dependia das ofertas do sistema bancário tradicional, mas com o progresso das tecnologias, das empresas e da sociedade, a evolução de ofertas é quase orgânica. Sai na frente quem fizer escolhas inovadoras e ao mesmo tempo seguras.

(*) - É CEO da Ulend, plataforma de crédito privado que conecta empresas, fundos investidores (www.ulend.com.br).

IGESP S/A - Centro Médico e Cirúrgico Instituto de Gastroenterologia de São Paulo

CNPJ/MF Nº. 61.442.190/0001-91

Edital de Convocação de Assembleia Geral Extraordinária

Ficam convocados os senhores acionistas do IGESP S.A. Centro Médico e Cirúrgico Instituto de Gastroenterologia de São Paulo a comparecerem no dia **24.05.2023** na Rua Silvia, 276 - 20º andar - no bairro da Bela Vista da Capital do Estado de São Paulo, para realização da **Assembleia Geral Extraordinária**, a fim de reunidos deliberarem sobre a seguinte ordem do dia: 1. Leitura, discussão e aprovação da redação da ata da Assembléia anterior; 2. Eleição Diretoria e Consellhos; 3. Outros Assuntos de interesse da Instituição. São Paulo, 10 de maio de 2023. **Fernando José Moredo** - Presidente.

Para informações detalhadas da certificação digital baixe o pdf e clique na assinatura

JORNAL EMPRESAS E NEGOCIOS LTDA:05687343000190

Assinado de forma digital por JORNAL EMPRESAS E NEGOCIOS LTDA:05687343000190
Dados: 2023.05.11 21:09:40 -03'00'

LEIA O QRCODE ABAIXO E ACESSE A PUBLICAÇÃO EM NOSSO PORTAL

https://jornalempresasenegocios.com.br/publicidade_legal/igesp-s-a-centro-medico-e-cirurgico/

Empresas & Negócios