OPINIÃO

2020: um ano para não ser esquecido

Enio Klein (*)

2020 foi um ano atípico. Um ano em que uma epidemia virou a sociedade e os negócios de ponta a cabeça. Mas não será um ano a ser esquecido

Ao contrário, deve ser lembrado como um período no qual muitos paradigmas foram quebrados e muitas lições foram e ainda hão de ser aprendidas. Desde temas sociais, de respeito ao próximo e solidariedade com os mais vulneráveis até negócios e o uso da tecnologia, 2020 será lembrado como um ano em que tivemos que reaprender comportamentos, mudar a maneira como trabalhamos e buscar novas soluções para os negócios.

2020 nos mostrou, mais do que nunca, que a vida de cada indivíduo pode depender do comportamento do outro. Desde o uso de máscara, o distanciamento social, evitar aglomerações e cuidar da higiene pessoal, até a ajuda com alimentos e equipamentos, percebemos, enquanto sociedade, que precisamos evoluir e melhorar muito a forma como nos relacionamos e respeitamos o próximo.

A crise também mostrou que as desigualdades sociais e de infraestrutura para o uso universal da tecnologia são grandes, tornando compulsória a abordagem do tema por parte dos formuladores de políticas públicas imediatamente. Tomando a educação como exemplo, com a quarentena e o fechamento das escolas, o ensino a distância foi a solução imediata. Contudo, o uso da tecnologia requer infraestrutura, equipamentos e conhecimentos que uma parte da sociedade não tem.

E viu-se o drama de o acesso à educação, durante a pandemia, como sendo praticamente impossível para essa parcela da população, que só dispõe de um telefone celular, uma rede precária e cara. No entanto, se olharmos o copo meio cheio, vimos que é possível ampliar o atendimento ao ensino usando a tecnologia, com políticas governamentais estabelecidas neste objetivo.

O mesmo se mostrou claro em relação à saúde, com o uso da telemedicina, sendo uma excelente opção de proporcionar atendimento médico eficiente a distância, além do benefício de solicitar exames e receitar medicações digitalmente. Pelo lado dos negócios, o Whatsapp e o Instagram foram usados como válvula de escape para muitos conseguirem manter seus negócios.

Com todos os seus inconvenientes e falta de segurança. Longe de ser nas condições ideais, a tecnologia apoiou pequenas ou até médias e grandes empresas nas operações comerciais. A barreira e o paradigma do uso da tecnologia foram quebrados e abriu-se um horizonte enorme para a modernização nessa área para empresas que sequer consideravam essa alternativa.

Em relação à forma de trabalhar, nos ambientes onde foi possível, as empresas mantiveram seus funcionários trabalhando em casa e o uso de aplicativos de vídeo conferência explodiu. Ainda não se estabeleceu a melhor equação entre qualidade de vida, segurança da informação e eficácia no trabalho remoto, mas, certamente, a rejeição que existia foi quebrada e, hoje, as empresas já pensam seriamente em mesclar este modelo com o trabalho presencial convencional como alternativa de custos mais baixos com benefícios aos empregados.

2020 foi o ano em que a tecnologia finalmente rompeu barreiras e, por necessidade, apresentou as suas credenciais como base para um pensamento de inovação e melhoria, tanto sob o aspecto social quanto dos negócios. E, afinal, são duas faces da mesma moeda. Negócios crescendo geram empregos que melhoram as condições sociais.

Precisamos e esperamos que os governos tenham percebido esse movimento tanto quanto as desigualdades e lacunas para que possamos ter maior acesso aos benefícios da tecnologia, cada vez mais universal. Precisamos também que esse movimento seja usado de forma menos oportunista pelos fornecedores de tecnologia, menos para cumprir suas metas de curto prazo, mas para incluir as organizações – empresas, ONGs, instituições de ensino – de qualquer tamanho no mundo digital.

Só assim, enquanto sociedade, criaremos também as condições de competitividade e resiliência em empresas de todos os portes, para que sejam longevas em sua missão de gerar emprego e renda, minimizando as desigualdades, ao mesmo tempo em que o país como um todo amplie suas capacidades de prever e enfrentar crises.

Essas são as lições de um ano que não devemos esquecer. Não pelas oportunidades que dizem que a crise cria, mas pelas lições inestimáveis que 2020 deixa para o nosso futuro.

(*) - Professor de Pós na Business School SP, especialista em Transformação Digital, em vendas, experiência do cliente e ambientes colaborativos, é CEO da Doxa Advisers.

Cinco formas da sua empresa ser invadida e como se prevenir

Especialista do Grupo Daryus chama a atenção para erros básicos que podem acontecer nas empresas, como a violação física de dados, e dá algumas dicas sobre como estar sempre alerta

Ao entender melhor como os hackers invadem os dados das empresas, especialistas já conseguem distinguir quais são as ameaças comuns que aumentaram significativamente nos últimos meses mesmo com a LGPD em vigor. Segundo o especialista e evangelista em Segurança da Informação e Proteção de Dados do Grupo Daryus, Cláudio Dodt, são duas as ameaças observadas com mais frequência nos últimos tempos:

Divulgação AI/Grupo Daryus

- Violação de Dados ou Data Breach: ocorre quando uma organização sofre um incidente de segurança relacionado aos dados pelos quais é responsável. Isso resulta numa violação de confidencialidade, da disponibilidade ou da integridade dos dados.

- Vazamento de Dados: transmissão não autorizada de informações de dentro de uma organização, ou seja, um incidente que expõe publicamente informações sensíveis que podem ser vistas, copiadas, roubadas, transmitidas ou usadas sem acesso autorizado.

Dodt destaca que investir em ferramentas de segurança, softwares de última geração e funcionários treinados são ótimas recomendações, porém isso não garante que a empresa não ficará vulnerável, uma vez que essas boas práticas se depreciam com o tempo e os criminosos se aperfeiçoam cada vez mais.

Confira as cinco maneiras que as organizações podem ser violadas e quais as possíveis soluções para os problemas:

Vulnerabilidades desconhecidas

A maioria das vulnerabilidades pode permanecer desconhecida por meses ou até anos. Esse foi o caso das vulnerabilidades de hardware encontradas pela equipe do Google chamadas de Meltsown e Spectre que permitem que os programas roubem dados processados pelo computador. A Meltdown é uma falha de segurança passível de ser explorada em microprocessadores. Ao explorar a falha é possível ler áreas de memória protegidas, ou seja, é possível obter dados sensíveis do usuário. A Spectre não afeta um processador específico, mas sim a maioria dos processadores. Com a falha é possível realizar "Branch Prediction" e "Speculative Execution". Através dela consegue-se fazer com que o processador execute instruções atípicas e assim fure o isolamento entre aplicações. Essas vulnerabilidades afetaram a memória da maioria dos hadwares de CPU nos últimos 10 anos e, embora não haja casos confirmados de exploração, isso não significa que criminosos não estejam aproveitando a vulnerabilidade.

Solução: seguir os conselhos básicos de segurança digital, pois não há outra forma ainda de lidar com falhas de seguranças desconhecidas.

Ameaça Interna

A ameaça interna nunca deve ser subestimada. Mesmo que não seja causada por um cibercriminoso, na maioria das vezes, a atenção deve ser mantida da mesma forma. Funcionários que não foram treinados adequadamente ficam propensos a erros acidentais, como enviar uma mensagem de e-mail para o destinatário errado, clicar em e-mails recebidos que contenham armadilhas de invasão – conhecidos como phishing -, até mesmo compartilhar informações confidenciais em um local público ou rede social. É importante considerar que existem pessoas que voluntariamente cometeriam uma violação ou até um crime. Por exemplo, um funcionário que pretenda deixar a empresa pode tentar copiar arquivos confidenciais, mesmo que seja contrário à política de segurança.

Solução: existem diversas formas para proteger a empresa de ameaças internas e remediar estragos causados caso algo aconteça. A organização pode realizar soluções endpoint como antivírus, controle de USB, sistemas de Data Leak Protection (DLP), além da contratação de uma equipe experiente de respostas a incidentes.

O risco de terceiros

Não muito diferente do tópico anterior, terceiros são pessoas ou empresas com as quais compartilhamos dados. É importante ressaltar que ao compartilhar informações, os terceiros ficam expostos aos mesmos riscos dos colaboradores da empresa e podem ser a porta para algum incidente. Para estes é necessário trabalhar dentro dos limites da organização, além dos controles de segurança já mencionados. É válido considerar regras especiais para pessoas de fora, como limitar as conexões à rede e servidores corporativos. Controles físicos também devem ser aplicados, incluindo a limitação do acesso a áreas restritas, o uso de crachás de identificação e a inspeção de mochilas e maletas, se necessário.

Solução: algumas formas de lidar com os riscos de segurança de terceiros é ter um aviso obrigatório de vazamento de dados, impor requisitos como criptografia e prevenção de vazamento de dados, além de contar com uma equipe de resposta a incidentes, e manter o direito de auditar a infraestrutura de terceiros.

Criptografia é uma faca de dois gumes

A criptografia é provavelmente um dos melhores controles de segurança, pois permite que dados confidenciais sejam transmitidos com segurança por redes não seguras. O problema é que também funciona na contramão. Como a maioria dos serviços da internet – navegação, mensageiros instantâneos, armazenamento de e-mail e nuvem – já impõe forte criptografia, torna-se difícil o controle dos dados que saem da empresa. Além disso, a criptografia pode ser adotada pelo malware para se comunicar com os servidores de comando e controle.

Solução: quando tudo está criptografado, a única solução é contorná-lo. As empresas com firewalls e proxies web mais antigos podem ter dificuldades, mas as soluções modernas já podem conter métodos de descriptografia, como inspeção SSL. Vale ressaltar que existem limitações em algumas situações. Algumas instituições financeiras, por exemplo, não funcionam bem com a inspeção SSL e pode haver preocupações com a privacidade. Portanto, nem sempre é possível descriptografar todo o tráfego dentro e fora da empresa.

Violação física

As vezes ela é esquecida, mas os dados não se limitam a bits e bytes. Uma violação também pode ocorrer com informações compartilhadas verbalmente, ouvidas por terceiros indesejados ou até por um documento impresso que foi deixado sem supervisão em algum local compartilhado por várias pessoas, por exemplo. Se um HD for descartado incorretamente, ele pode acabar na mão de cibercriminosos que podem tentar restaurar as informações e usá-las de forma negativa.

Solução: ter uma política de mesa limpa, usar meios seguros para descartar informações confidenciais e fornecer treinamento de conscientização dos funcionários são as melhores opções nesse caso.

News @TI

ricardosouza@netjen.com.br

Plataforma brasileira de gestão de tempo e produtividade

@Ampliando seu portfólio de soluções inovadoras que ajudam a transformar dados em informação de valor, a Meeta Solutions, empresa de tecnologia 100% brasileira, está lançando a primeira plataforma em nuvem para gestão de tempo e produtividade, desenvolvida no Brasil com foco em trazer equilíbrio entre a vida profissional e pessoal. Denominada Evertrack, a plataforma permite acompanhar as atividades das equipes e informações em real time, ajudando gestores e colaboradores a gerir sua jornada de trabalho e fazer melhor uso do investimento de tempo. César Garcia, CTO da Meeta Solutions, explica que há muito discute-se produtividade no ambiente de trabalho. Mas, diante desse novo "normal" e da forma como o home office se impôs, essa questão veio mais à tona, tornando uma necessidade para todo tipo de organização (https://evertrack.com.br/?utm_source=PR_plataforma%20_evertrack&utm_campaign=PR_plataforma%20_evertrack).

Fundadora do Nubank e presidente da Microsoft Brasil participam do AAA Summit

@Cristina Junqueira, cofundadora do Nubank, e Tânia Cosentino, presidente da Microsoft Brasil, confirmaram presença no AAA Summit, evento 100% online e 100% gratuito, que vai reunir os maiores especialistas do país com palestras sobre o que esperar de 2021. A ideia é decifrar as visões de algumas das maiores autoridades de negócios do Brasil sobre empreendedorismo, gestão, inovação e comportamentos. Será no dia 20 de janeiro de 2021 com um grupo selecionado de palestrantes com visões únicas sobre as grandes tendências que vem por aí. A estimativa é que participem 50 mil empresários, executivos e profissionais interessados em gestão, liderança, empreendedorismo, inovação, economia, tendências e futuro.

Empresas & Negócios **José Hamilton Mancuso (1936/2017)**

Publisher: **Lilian Mancuso** (lilian@netjen.com.br)

Editorias

Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: Tatiana Sapateiro – tatiana@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza. *Revisão:* Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Jornal Empresas & Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080 – Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br) – Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90 - JUCESP, Nire 35218211731 (6/6/2003) - Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

RIO DE JANEIRO: **J.C. REPRESENTAÇÕES E PUBLICIDADES EIRELI**
Av. Rio Branco, 173 / 602 e 603 – Centro - Rio de Janeiro - CEP 20040-007
Tel. (21) 2262-7469 – CNPJ 30.868.129/0001-87