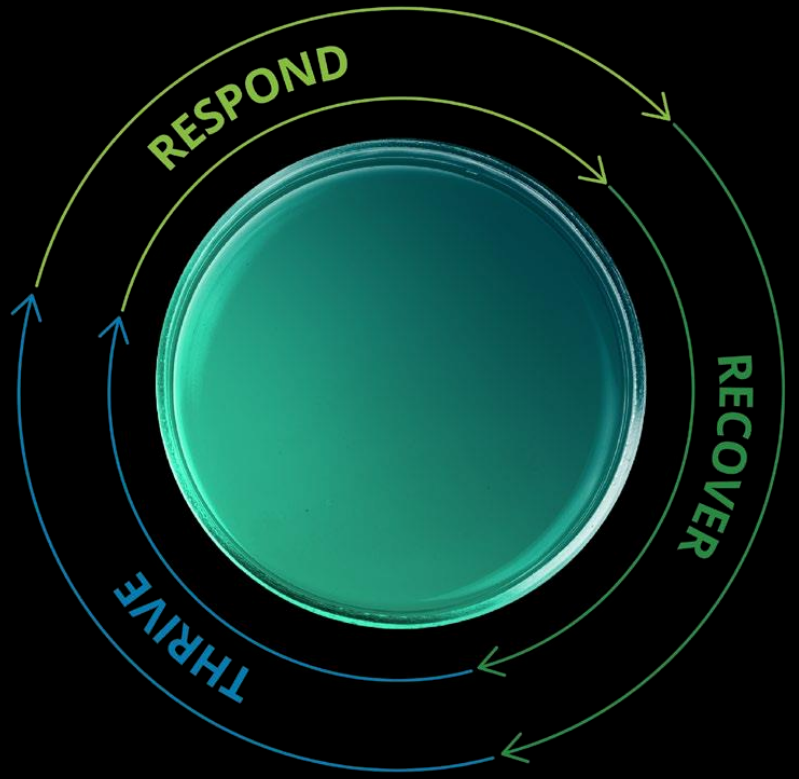
Deloitte.



COVID-19: Cibersegurança e força de trabalho remota

Frederico Macias

MAKING AN IMPACT THAT MATTERS since 1845

COVID-19: Cibersegurança e força de trabalho remota

De que forma as vulnerabilidades de cibersegurança, por um lado, e a eficiência operacional, por outro, vão continuar a remodelar o "próximo normal"?

O furacão causado pela pandemia: *respond*

De uma forma quase instantânea, as empresas a nível global foram colocadas em situações de desconexão física aos seus escritórios, em que os colaboradores tiveram que se isolar e trabalhar de forma remota. Este contexto criou uma pressão extra nas áreas de cibersegurança, de entre as quais destacamos algumas dimensões:

- **Explosão "BYOD – Bring your own device"** – Muitos colaboradores não tinham dispositivos (ex.: laptops ou smartphones) atribuídos pela empresa para uso off-site no momento do confinamento. Isto significa que nalguns casos assistimos a acessos a redes e a sistemas corporativos em dispositivos que podem ter vulnerabilidades ou estão à priori comprometidos. Da mesma forma, uma parte significativa dos colaboradores confiam em ferramentas de conferência e colaboração para executar as suas tarefas, e que podem ser facilmente comprometidas sem cuidados adicionais de proteção, por atores de ameaças. Tudo isto aumentou significativamente a complexidade de segurança devido à expansão brusca da superfície de ataque típica das organizações.

- **Ambiente de computação remoto** – As organizações não têm controlo sobre o ambiente de computação remoto dos seus colaboradores. Os problemas que daí emergem vão desde colaboradores com dificuldade em trabalhar em pequenos locais, ou com pouca privacidade, até colaboradores cuja largura de banda é insuficiente para oferecer o desempenho aceitável para videoconferências, por exemplo. E, comna realidade “IoT – Internet of Things”. podemos ter, na mesma rede doméstica vários aparelhos ligados, desde TV’s até outros aparelhos, temos um ambiente fértil em vulnerabilidades. Para um verdadeiro futuro "trabalho remoto", as equipas envolvidas nas definições de cibersegurança precisam de implementar programas e protocolos que reduzam os riscos nesses ambientes e não comprometam a eficiência operacional.

- **Acesso remoto seguro** – A maioria das empresas simplesmente não estava pronta para um mundo onde a maioria dos colaboradores têm acesso remoto seguro às aplicações corporativas. Nas organizações que dependem de sistemas legacy o impacto é maior porque estes sistemas são propensos a problemas de desempenho, escalabilidade e disponibilidade. E se os colaboradores transitaram para o uso de dispositivos da sua escolha, também devem entender e respeitar as políticas adequadas de “higiene” e segurança corporativa. Neste contexto, as equipas de cibersegurança devem adotar modelos de confiança zero, suportados em componentes fortes de identidades e acessos, e em que possam detetar e responder a comportamentos anómalos.

- **A ameaça interna** – Os ambientes de competitividade económica continuarão a contribuir para um aumento no volume de ameaças internas. As Lideranças devem assegurar que as suas organizações estão preparadas para prosseguir um programa de identificação de ameaças internas baseadas em riscos. Consciente ou inconscientemente, a maioria dos incidentes de cibersegurança são causados por um funcionário da organização impactada. Em muitos casos estes comportamentos arriscados seriam evitáveis.

- **Processos "ad hoc" inseguros** – Foram executados processos de desenvolvimento rápidos para suportar esta nova realidade ou mesmo para aumentar o volume de negócios em canais digitais, que infelizmente num número significativo de organizações não passaram por nenhuma validação da área de cibersegurança. Foram colocados em produção sem uma validação prévia, com o risco acrescido de, nalguns casos, serem executados em ambientes domésticos distribuídos e potencialmente inseguros. Ainda que esta nova realidade venha reforçar a urgência de digitalizar processos de negócio, a curto/médio prazo isso significa que as equipas de cibersegurança deverão ser capazes de incorporar ciclos de segurança e conformidade nestes novos processos: autenticar identidades, garantir acesso seguro à documentação de suporte (muitas vezes confidencial) e garantir o cumprimento, entre outras, de legislação de privacidade e proteção de dados pessoais… em muitos casos,a partir de dispositivos que não foram atribuídos pelas organizações. Não há nenhum roteiro pré-definido com tudo o que deve ser feito. É uma situação nova, é necessário pensar o contexto de cada negócio e processo para se executar da forma mais eficiente e eficaz.

COVID-19: Cibersegurança e força de trabalho remota

De que forma as vulnerabilidades de cibersegurança, por um lado, e a eficiência operacional, por outro, vão continuar a remodelar o "próximo normal"?

Recuperação “pós-pandemia”: *recover*

As organizações, ainda que em estágios de maturidade distintos, estão a preparar-se para o mundo “pós-pandemia”, onde a habilitação e a produtividade remotas dos colaboradores são e serão parte integrante dos seus planos. À medida que institucionalizam estes novos processos e funções, a cibersegurança deveria ser um player determinante em todos os sentidos e esforços. Quando a cibersegurança é incorporada no conteúdo das discussões estratégicas e no design aplicacional, trabalhamos todos para que o "próximo normal" não se torne na “próxima fonte de risco”. Adicione-se um fator importante: é muito menos oneroso incluí-la no inicio do que no fim do ciclo de vida de produção das aplicações.

A recuperação da situação em que nos encontramos não será rápida. Será um processo gradual de regresso, que nalguns casos será seguramente adequado a cada tipo de negócio, operação, geografia, faixa etária, tipo de responsabilidade, entre outros fatores. Nas organizações que englobem vários dos fatores mencionados, esta multiplicidade de cenários e de ambientes híbridos forçá-las-á, e em especial às suas equipas de cibersegurança, a adotar novos níveis de agilidade para se adaptarem a este ambiente modular e assegurarem níveis de risco baixos e controlados. Isto levantará desafios consideráveis, seguramente.

COVID-19: Cibersegurança e força de trabalho remota

De que forma as vulnerabilidades de cibersegurança, por um lado, e a eficiência operacional, por outro, vão continuar a remodelar o "próximo normal"?

Uma visão próspera para o futuro: *thrive*

Até há algum tempo atrás as organizações dedicavam a maior parte dos seus investimentos em tecnologia e segurança na geração de receita e eficiência operacional. E era natural que assim fosse, uma vez que essas são geralmente as principais prioridades de uma organização. O mundo "pós-pandemia", no entanto, poderá ver um reequilíbrio de recursos em direção à resiliência corporativa, focado na segurança, para maiores capacidades de trabalho remoto num futuro que já nos bate à porta.

Existem muitos caminhos a percorrer. Ficam apenas alguns, de entre muitos, que as organizações podem adotar ou mesmo repensar no sentido de criarem os mecanismos de adaptação a este novo cenário:

- Assegurar que as equipas de Tecnologias de Informação implementam as políticas e diretrizes de segurança corporativa para o "BYOD – Bring your own device" e que os diversos componentes de segurança corporativa indicados pelas equipas de cibersegurança sejam instalados nos dispositivos dos colaboradores que os desejem conectar às redes corporativas. Existem mecanismos que permitem assegurar esta instalação e update sempre e quando estes se conectam a estas redes.

- Rever e adequar as regras de firewalls corporativas para acesso remoto, monitorizar e analisar os Comportamentos de Utilizadores e Entidades (UEBA), monitorizar a integridade de ficheiros e controlar os processos de acesso e utilização das ferramentas e aplicações corporativas.

Os caminhos acima mencionados irão impulsionar o interesse renovado em tecnologias que permitam acesso remoto seguro e, acima de tudo, a tão desejada produtividade, e que não tem sido simples de alcançar nas fases de resposta e recuperação:

- "**VDI – Virtual Desktop Infrastructure" e "DaaS – Desktop as a Service".**

Reduzirá em muito os problemas causados por utilizadores que utilizam dispositivos não aprovados para aceder a ativos de computação corporativa, permitindo que as equipas de cibersegurança e de Tecnologias de Informação façam uma gestão centralizada dos dispositivos dos utilizadores, dando-lhes um controlo muito mais alargado e profundo do que o possibilitado pelos acessos tradicionais. Esta tecnologia existe desde o início dos anos 2000, mas demorou a ganhar preponderância devido a problemas de complexidade e desempenho. Hoje, no entanto, com as ofertas de VDI baseadas em nuvem, uma parte significativa destas limitações foram amplamente ultrapassadas, transformando-as em tecnologias poderosíssimas no futuro do trabalho remoto.

- **"IAM – Identity and Access Management".**

Também esta tecnologia teve problemas de adoção resultantes de custos e complexidade de implementação. O aparecimento de soluções de IAM baseadas em cloud reduziu drasticamente a complexidade técnica e tornou a sua implementação mais eficiente e transversal a toda a empresa, em especial se considerarmos que existe uma transposição gradual de aplicações para ambientes cloud. As organizações também podem procurar fornecedores de identidade digital para habilitar e gerir este processo. Em muitos casos com maior eficácia e menor custo global para a organização. Resta dizer algo que é preponderante: o IAM é central para a adoção de uma arquitetura de confiança zero, que será exigida pela maioria das organizações que ambicionam gerir adequadamente o risco com uma força de trabalho remota em larga escala.

- **Cloud computing.**

A migração para a Cloud, tantas vezes "congelada", pode ganhar maior velocidade neste cenário de colaboração remota. Uma parte significativa das organizações que dependem de sistemas legacy continuarão a enfrentar problemas de desempenho, escalabilidade e disponibilidade com sua infraestrutura local. Muitas vezes estes problemas têm sido resolvidos de forma temporária com custos avultados em comunicação e licenciamento de software adicional/complementar. Nalguns casos estes custos adicionais (ex.: em falta de produtividade) acelerará a migração destes sistemas para a Cloud (privada, publica ou hibrida, em função das necessidades específicas de cada tipologia de negócio). É uma oportunidade única para as organizações envolverem as equipas de cibersegurança como uma componente crucial do processo para garantir que todas as considerações, benefícios e riscos, são devidamente ponderados e implementados.

As organizações "nativas da Cloud" saíram rapidamente da fase de "respond". Já tinham adotado e embebido parte ou totalidade das tecnologias mencionadas, pelo que a mudança para um modelo de força de trabalho 100% remota foi um passo relativamente simples. As organizações que mais lutam são as que adiaram a necessidade de amadurecer a sua postura de cibersegurança de forma transversal aos seus processos.

COVID-19: Cibersegurança e força de trabalho remota

De que forma as vulnerabilidades de cibersegurança, por um lado, e a eficiência operacional, por outro, vão continuar a remodelar o "próximo normal"?

O Futuro das Pessoas, Processos e Tecnologia

O desempenho corporativo é impulsionado por pessoas, processos e tecnologia. Este triângulo dever ser trabalhado de forma conjunta para executar efetivamente a transformação digital necessária e permitir assim um ambiente onde a força de trabalho remota seja um processo natural no seio das organizações. E ainda que não venha a ser seguramente exclusivo, porque há processos que o digital ainda não substitui, passará forçosamente a fazer parte do novo dia-a-dia das organizações.

A postura de cibersegurança das organizações pode naturalmente melhorar como resultado deste processo forçado de transformação. As funções mais basilares da cibersegurança como patching, gestão de vulnerabilidades e programas de formação e consciencialização, entre outros, podem seguramente tornar-se, estas sim, no “novo normal”. A oportunidade surge se aprendermos todos com as lições do passado e as transformarmos na próxima geração de capacidades organizacionais de cibersegurança.

Tecnologia

Acesso controlado, áreas de trabalho virtuais, gestão de dispositivos remotos e sistemas e aplicações escaláveis em cloud serão críticos para permitir a transição segura dos ambientes tradicionais de escritório para os ambientes híbridos onde o remoto ganhará preponderância.

Pessoas

As pessoas e as suas identidades digitais precisam de ser "confiáveis, mas verificadas" para desempenhar as suas funções num ambiente remoto adequado e sem supervisão direta, garantindo em paralelo a conformidade com as políticas de cibersegurança adequadas.

Processos

Qualquer processo que exija interação física deve ser avaliado e, sempre que possível, digitalizado para permitir a execução segura do processo num ambiente de trabalho remoto.

Contato:

Frederico Macias
Partner Risk Advisory
D:+351 210422500
fremacias@deloitte.pt