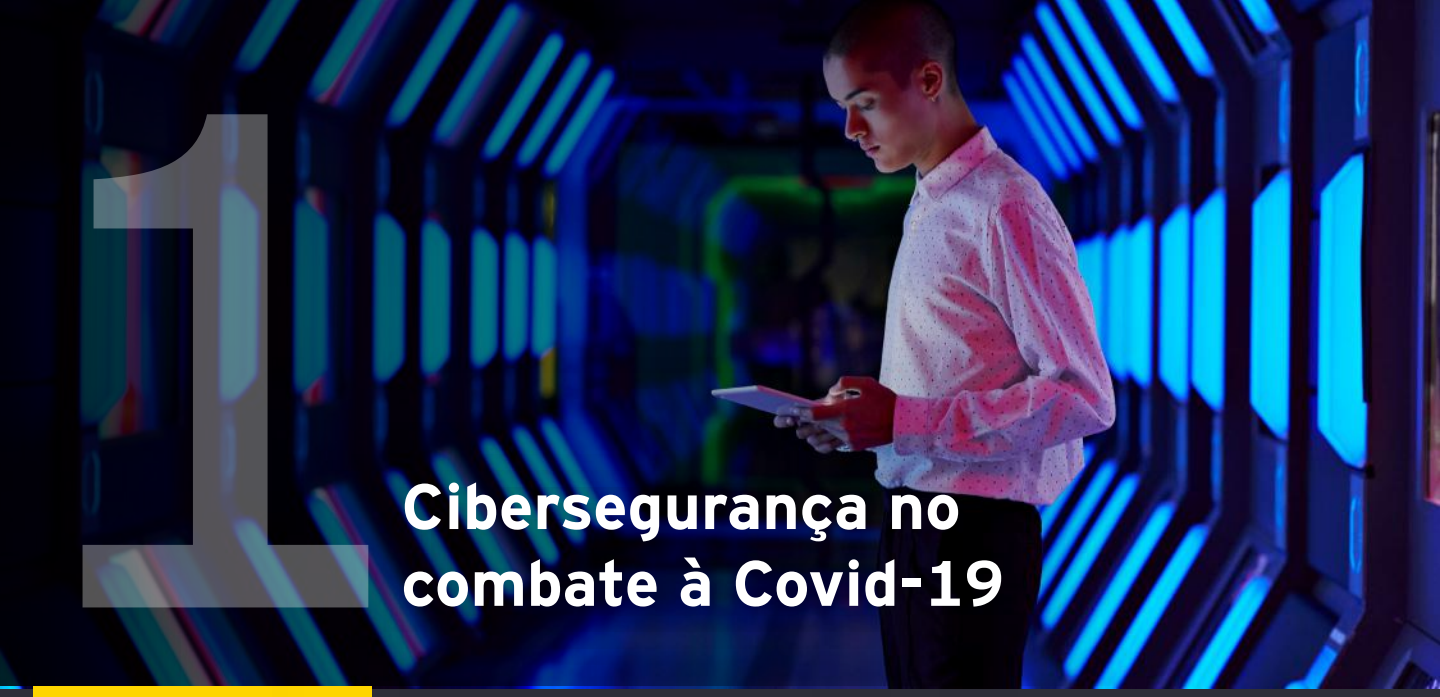
Cibersegurança contra a Covid-19

Transformando cibersegurança e privacidade em agentes estabilizadores no combate à pandemia da Covid-19

Abril 2020

Publicação de Cibersegurança
EY Brasil

Building a better working world



1 Cibersegurança no combate à Covid-19

Demetrio Carrión
Sócio-Líder Cibersegurança LAS & Brasil

São Paulo, Brasil

demetrio.carrion@br.ey.com

www.linkedin.com/in/demetriocarrion

7 formas de usar a cibersegurança como fator de estabilidade durante a pandemia – e como garantir a privacidade

A pandemia causada pelo novo coronavírus mudou o mundo em poucas semanas e as prioridades de governos, empresas e da sociedade foram revistas.

Mas, como Peter Drucker dizia, não podemos confundir movimento com progresso.

No afã de agir sem deliberar, podemos involuntariamente criar crises dentro da crise. Definir soluções para clientes de forma equivocada, prometer soluções que não operam como esperado, contratar serviços sem o mínimo de avaliação são apenas alguns exemplos de como aumentar a instabilidade.

Neste momento, a sociedade vem lutando em diversos *fronts*. Agir nesses *fronts* é fundamental, assim como protegê-los para que eles deem os resultados esperados.

O *front* que protege *fronts* se chama cibersegurança. Soluções que não sejam *Security by Design* e *Privacy by Design* aumentam a entropia. Essa entropia aumenta o caos e cria novos focos de incêndio. Neste momento, promover o máximo de estabilidade possível é fundamental.

Um pé no acelerador e um bom controle das marchas são fundamentais para que percorramos esta jornada na velocidade correta e com o torque adequado.

O Fórum Econômico Mundial publicou em sua página web um artigo chamado *Why cybersecurity matters more than ever during the coronavirus pandemic* [1] corroborando com a visão estabilizadora de cyber.

Cyber deve ser habilitador do negócio, tanto na construção de novos serviços como na garantia da sua perenidade.

Nesta publicação, discutiremos sete pontos de vista sobre como cyber pode ser utilizado de forma a trazer equilíbrio neste momento de incerteza. Esses pontos de vista foram organizados da seguinte forma:

1. Segurança, Riscos, Conformidade e Resiliência
2. Proteção de Dados e Privacidade
3. Gestão de Acessos e Identidades
4. Arquitetura, Engenharia e Tecnologias Emergentes
5. Próxima Geração de Operações e Resposta de Segurança
6. Cyber em Tecnologia de Automação
7. Pandemia de Ameaças Cibernéticas

Esta publicação está muito longe de ditar pontos de chegada. Ela foi criada tendo a empatia em primeiro lugar. É uma forma de nos colocarmos na perspectiva de cada um dos leitores para poder servi-los, oferecendo potenciais pontos de partida para essa jornada.

1 www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

Autores

Demetrio Carrión, MSc, CISSP, CISM, CISA, CRISC, PMP
Sócio-líder de Cibersegurança LAS & Brasil

Alex Aguiar, MBA
Sócio de Cibersegurança Brasil

Rinaldo Ribeiro, CISSP, CIPP/E
Sócio de Cibersegurança Brasil

Raphael Gomes, CISSP, CISM, CISA, CRISC, GCFA
Associate Partner de Cibersegurança Brasil

Bruno Dutra, CBCP, BS 25999 LA
Gerente Sênior de Cibersegurança Brasil

Fábio Isaguirre
Gerente Sênior de Cibersegurança Brasil

Luana Oliveira, EXIN PPDF, ISO 270001 LA, CobIT F
Gerente Sênior de Cibersegurança Brasil

Waldemar Magalhães
Gerente Sênior de Cibersegurança Brasil

Contribuiu

Marcos Sêmola CISM, EXIN PPDF, ISO27001 LA
Sócio de Cibersegurança Brasil

2 Segurança, riscos, compliance e resiliência

Demetrio Carrión
Sócio-Líder Cibersegurança LAS & Brasil

São Paulo, Brasil

demetrio.carrion@br.ey.com

www.linkedin.com/in/demetriocarrion

Novos tempos requerem novas soluções? Atuar em estado de emergência requer esquecer o passado e o aprendizado e criar tudo do zero?

Sempre há espaço para a inovação, mas nunca deve haver espaço para o improviso em momentos de crise. Inovação e invencionice são coisas diferentes. Mas, na correria, podem parecer a mesma coisa.

O mundo já passou por situações extremas e há muito conhecimento produzido para os momentos de estabilidade e para os momentos de turbulência. Isso é aplicável em larga escala em cibersegurança e privacidade.

Há um amplo leque de *frameworks*, modelos, soluções que já foram comprovados como eficientes e eficazes ao longo dos tempos.

O NIST CSF *(Critical Infrastructure Framework)* é um grande exemplo de um *framework* já consagrado e que deve ser alavancado neste momento. O NIST contribui com uma visão ampla de cyber e é baseado em riscos.

Outros modelos e padrões podem ser citados, como ISF *(Information Security Forum),* ISO 27001/2, o recém-publicado CyBOK, dentre outros.

Esses e outros modelos são bússolas para nos guiar neste momento difícil. Devemos utilizar esse conhecimento como norte do que deve ser priorizado e sempre de forma interligada.

É urgente e reconfortador utilizar estes *frameworks* pelos seguintes motivos, que podem ser lembrados pelo acrônimo 5C.

- São **Comprovados**, porque foram implementados inúmeras vezes e com sucesso;
- São **Consagrados**, porque são utilizados mundialmente;
- São **Criteriosos**, porque são orientados por riscos;
- São **Construtivos,** porque buscam eliminar o máximo possível os pontos cegos, dado que são abrangentes e instrutivos;
- São **Conectores**, porque possuem uma linguagem comum e integradora.

Bruno Dutra
Gerente Sênior
de Cibersegurança

Rio de Janeiro, Brasil

bruno.dutra@br.ey.com

www.linkedin.com/in/brunoadutra

Seção especial: resiliência

Na física, a resiliência é a propriedade que alguns materiais possuem de retornar à forma original após terem sido submetidos a uma deformação. Em um sentido figurado, podemos dizer que resiliência é a capacidade de se adaptar às mudanças.

É em momentos de crise que nos lembramos das coisas que realmente importam e aprendemos na prática o que significa resiliência. Isso vale tanto para nossa vida profissional como para nossa vida pessoal.

É uma pena que muitas pessoas e muitas empresas só parem para atentar sobre a relevância de vários temas como epidemias e pandemias, vide a da Covid-19, que vivenciamos atualmente, quando chegam à porta de nossas casas.

Se sua empresa se preparou, ótimo, agora é hora de validar o seu plano de contingência. Porém, muitos dos impactos que poderiam ser minimizados são agravados por falta de preparo adequado.

Apesar disso, mesmo que o preparo não tenha sido pensado anteriormente, conforme as boas práticas indicam, não podemos deixar que as crises cresçam e se tornem cada vez maiores até o ponto de perdermos o controle.

Pensando nisso, o que os líderes devem fazer agora?

1. Comunique-se com seus funcionários para aumentar a conscientização, aplicar políticas (por exemplo, restrições de viagem, home office etc.) e familiarizá-los com as ferramentas e os recursos disponíveis na empresa;

2. Informe seus parceiros, prestadores de serviços e terceirizados sobre as ações que deverão ser tomadas para se adequarem às medidas adotadas pela empresa;

3. Revise as estratégias relacionadas à Gestão de Continuidade de Negócios (GCN) e, caso não tenha sido contemplado cenário relacionado à pandemia, atualize-as;

4. Revise seus Planos de Gestão e Comunicação de Crises atualizando contatos com autoridades locais, nacionais e globais, bem como outras partes interessadas internas e externas;

5. Verifique se os funcionários possuem os recursos necessários, incluindo acesso a unidades de compartilhamento, acesso à VPN ou outras ferramentas importantes para executar tarefas críticas de forma remota;

6. Caso não tenha sido criado, monte um Comitê de Crises multidisciplinar e com as alçadas necessárias, para que ações emergenciais possam ser, rapidamente, discutidas e deliberadas;

7. Solicite aos funcionários que confirmem ou atualizem seus contatos, pois caso necessário os funcionários poderão ser rapidamente localizados;

8. Caso não possua, construa seu Programa de Gestão de Continuidade de Negócios. Se já o possui, é hora de exercitá-lo e revisá-lo com afinco.

3 Privacidade e proteção de dados e privacidade

Luana Oliveira
Gerente Sênior de Cibersegurança

São Paulo, Brasil

luana.oliveira@br.ey.com
www.linkedin.com/in/luana-oliveira-cyber

Governos, bem como organizações públicas, privadas e voluntárias, estão tomando as medidas necessárias para conter a disseminação e mitigar os efeitos da Covid-19. Muitas dessas etapas envolvem o processamento de dados pessoais (como nome, endereço, local de trabalho, detalhes da viagem) de indivíduos, incluindo em muitos casos dados pessoais sensíveis de "categoria especial" (como dados relacionados à saúde).

A lei de proteção de dados não impede o fornecimento de cuidados de saúde e o gerenciamento de problemas de saúde pública. No entanto, há considerações importantes quando lidar com dados pessoais nesses contextos, particularmente saúde e outros dados sensíveis.

Mesmo nossa lei ainda não estando vigente e a nossa Agência Nacional de Proteção de Dados não estar atuando no sentido fiscalizatório, o MPDFT vem sendo bem ativo em casos relacionados ao uso possivelmente abusivo de dados pessoais. Prevenir é sempre o melhor remédio, inclusive no âmbito legal!

Levar em consideração os princípios de qualquer lei de proteção de dados pessoais:

Legalidade

Existem várias bases legais para o processamento de dados pessoais nos termos do Artigo 11 da LGPD e condições que permitem o processamento de Categorias Especiais de dados pessoais, como dados de saúde, nos termos do Artigo 7, que podem ser aplicáveis neste contexto. Entre estes, o seguinte pode ser relevante.

Em circunstâncias em que as organizações estejam agindo sob a orientação ou instruções das autoridades de saúde pública ou de outras autoridades relevantes, é provável que o Art. 11 – II – (f) (g) e Art.13 permitam o processamento de dados pessoais, incluindo dados de saúde, uma vez implementadas salvaguardas adequadas. Tais salvaguardas podem incluir limitações no acesso aos dados, prazos estritos para apagamento e outras medidas, como treinamento adequado da equipe para proteger os direitos definidos na LGPD.

Os empregadores também têm uma obrigação legal de proteger seus funcionários sob a Lei de Segurança, Saúde e Bem-Estar no Trabalho. Essa obrigação fornece uma base legal para o tratamento de dados pessoais, incluindo dados de saúde, quando considerados necessários e proporcionados. Todos os dados processados devem ser tratados de maneira confidencial, ou seja, qualquer comunicação com a equipe sobre a possível presença de Covid-19 no local de trabalho geralmente não deve identificar empregados individuais.

Também é permitido processar dados pessoais para proteger os interesses vitais de um titular de dados individual ou de outras pessoas, quando necessário. Os dados de saúde de uma pessoa podem ser processados a esse respeito quando eles são física ou legalmente incapazes de dar seu consentimento. Isso geralmente se aplica apenas a situações de emergência, nas quais nenhuma outra base legal pode ser identificada.

Transparência

As organizações que processam dados pessoais devem ser transparentes quanto às medidas que implementam nesse contexto, incluindo o objetivo de coletar os dados pessoais e por quanto tempo serão retidos. Eles devem fornecer aos indivíduos informações sobre o processamento de seus dados pessoais em um formato conciso, facilmente acessível, fácil de entender e em linguagem clara.

Confidencialidade

Qualquer processamento de dados no contexto de prevenção da propagação da Covid-19 deve ser realizado de maneira a garantir a segurança dos dados, principalmente no que diz respeito aos dados de saúde. A identidade dos indivíduos afetados não deve ser divulgada a terceiros ou a seus colegas sem uma justificativa clara.

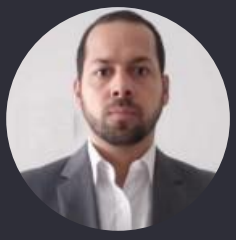
Minimização de dados

Como em qualquer processamento de dados, apenas a quantidade mínima necessária de dados deve ser processada para atingir o objetivo de implementar medidas para impedir ou conter a propagação do novo coronavírus.

Prestação de contas

Os controladores também devem garantir que documentem qualquer processo de tomada de decisão em relação às medidas implementadas para gerenciar a Covid-19, que envolvem o processamento de dados pessoais.

4 Gestão de acessos e identidades



Waldemar Magalhães
Gerente Sênior
de Cibersegurança

Rio de Janeiro, Brasil

waldemar.magalhaes@br.ey.com

www.linkedin.com/in/waldemar-esteves-magalhães-neto-4841a015

Com a intenção de minimizar a proliferação da Covid-19, empresas e organizações estão tomando ações sem precedentes. O trabalho remoto, ou teletrabalho, está se tornando padrão e uma solução de Gestão de Identidades e Acessos pode minimizar o risco de ações indevidas durante a crise que estamos enfrentando.

Abaixo seguem algumas ações emergenciais:

- Acessos críticos e privilegiados: antecipar ciclos de revisão de acesso para aplicações críticas ao negócio, incluindo restrição de horários para o usuário acessar a aplicação e, se possível, utilizar ferramentas que realizam gestão de acessos privilegiados por meio de controle de sessão;
- Aplicações *mobile*: priorizar integração de aplicações *mobile* à ferramenta de Gestão de Identidades e Acessos para minimizar o risco de vazamento de dados por meio de dispositivos sem as devidas credenciais;
- Segurança no *reset* de senha: incluir validação por meio de OTP (*One-Time Password*) ou controle similar para garantir que o usuário devido está realizando a modificação na senha;
- Autenticação multifatorial: caso a empresa possua uma ferramenta de MFA (*Multi-Factor Authentication*), ampliar a funcionalidade para utilização de todas aplicações que possuem acesso externo ou na nuvem;
- Análise de comportamento: utilizar a funcionalidade de análise comportamental para identificar anomalias e acessos indevidos.

Importante nesse momento priorizarmos medidas preventivas, com esforço relativamente baixo e com alto valor agregado para segurança da empresa.

5 Arquitetura e tecnologias emergentes

Rinaldo Ribeiro
Sócio de Cibersegurança

Rio de Janeiro, Brasil

rinaldo.ribeiro@br.ey.com

www.linkedin.com/in/rinaldo-ribeiro-de-oliveira-ba192

Nassim Nicholas Taleb, renomado autor libanês-americano, escreveu em 2007 o livro *Black Swan: The Impact of the Highly Improbable* (lançado em português como a *Lógica do Cisne Negro*) em analogia à crença de que até 1697 só existiam cisnes brancos, até um cisne negro ser visto na Austrália.

Muitas vezes, ao analisarmos ameaças de cibersegurança, deparamos com indivíduos que ignoram a importância de se considerar eventos *black swan*, aqueles com altíssimo impacto e baixa probabilidade de ocorrência. Às vezes, insistem em desprezar a necessidade de um preparo adequado para garantia da resiliência dos negócios, pautados na inexistência de uma análise de risco adequada.

Poderíamos considerar a incidência da Covid-19 e seu impacto crescente e devastador em todo o mundo como um *black swan*? Quais reflexões devemos fazer sobre a necessidade de sermos ágeis ao nos adaptarmos à nova realidade sem comprometer a cibersegurança e privacidade?

Adapte com segurança

Com a migração repentina para o trabalho remoto em massa, algumas organizações podem não ter ambientes tecnológicos preparados. Nesse movimento, modificações na arquitetura, seja na adoção de novos serviços na nuvem ou na disponibilização de aplicações externamente, podem levar a exposições indesejadas, alargando a janela de oportunidades para ataques e acessos indevidos.

Níveis de autenticação compatíveis com a criticidade das aplicações e controles de acesso adequados são exemplos de aspectos importantes a serem considerados.

Inovação e tecnologias emergentes com análise de riscos adequada

A agenda de inovação continuará acelerada e a adoção de tecnologias emergentes mais do que nunca se torna uma realidade. A crise mundial causada pelo novo coronavírus, levando à escassez de recursos humanos em certos processos críticos de negócio, pode realçar a importância de implementação de novas tecnologias.

Não necessariamente haverá uma mudança radical e repentina, mas muitos líderes irão analisar com mais atenção os benefícios de tecnologias emergentes em situações semelhantes. Imaginem um cenário ilustrativo em que existe automatização de processos usando inteligência artificial disponibilizada por terceiros com sistemas na nuvem.

Novamente, o lembrete é para explorar o que há de melhor no ganho produtivo na adoção desses cenários sem desprezar a importância de controles robustos de cibersegurança.

"*Situational awareness*" ou "Consciência situacional" aplicada à cibersegurança

Diante do cenário atual de rápida transformação, se torna essencial a percepção nítida de elementos e eventos à nossa volta, assim como a compreensão de seus significados e possíveis projeções futuras. Quando aplicado à cibersegurança, esse conceito de "consciência situacional" significa o entendimento mais claro das ameaças relevantes, assim como as motivações de possíveis agentes maliciosos que possam explorar o momento de incertezas para lançar novos ataques cibernéticos contra nossas organizações.

Nesse sentido, dois aspectos se tornam evidentes: colaboração no compartilhamento de informações relevantes e "*threat intelligence*" ou "inteligência de ameaças". O primeiro, quando feito de forma controlada e segura, é ferramenta poderosa na aceleração de capacidade de detecção e resposta a incidentes. O segundo capacita nossos times de cibersegurança a estarem "um passo à frente", quando as técnicas e formas de ataques cibernéticos são entendidas e aplicadas de forma proativa.

Ainda há tempo: proteção e revisão

Focando primeiramente e principalmente na proteção de vidas, antes da proteção dos negócios, adotamos mundialmente distanciamento social e cuidados essenciais de higiene redobrados. O momento gera incertezas e coloca à prova a capacidade de muitas organizações de reagirem e se adaptarem de forma eficaz. Excelente oportunidade para revisar os planos de continuidade de negócio, mas, principalmente, os planos de respostas a incidentes. Sim, os de cibersegurança!

6 Próxima geração de operações e resposta de segurança

Fábio Isaguirre
Gerente Sênior de Cibersegurança

São Paulo, Brasil

fabio.isaguirre@br.ey.com
www.linkedin.com/in/fabioisaguirre

O monitoramento de segurança e a resposta a incidentes são postos à prova durante a pandemia. É a primeira vez que tais disciplinas encontram um mundo em escala exponencial de dados, processamento e globalização, ao mesmo tempo que todas as regras do jogo mudam sem as empresas e nações terem se antecipado.

Compartilho alguns pontos de vista sobre essa temática a seguir.

Dissemine uma cultura de segurança

Alerte seus colaboradores para o risco de recebimento de e-mails de *phishing* associados ao coronavírus (Covid-19), avisos do Ministério da Saúde, paralizações e/ou associados ao trabalho remoto. Após comunicação formal, a empresa também pode executar ou contratar uma campanha, para medir o grau de conscientização de segurança da companhia.

Mantenha o monitoramento de segurança da infraestrutura tecnológica de forma contínua

A conscientização é importante e necessária, mas sozinha não é suficiente. Lembre-se de que o trabalho remoto exige cuidados especiais por parte do usuário final. Conexões a redes wireless desprotegidas (Wi-Fi público) ou o uso de computadores sem os softwares mínimos de segurança instalados e atualizados podem ser os elos fracos para um atacante invadir sua empresa.

Nesse sentido, o mercado de segurança provê serviços de segurança gerenciados, como, por exemplo, o serviço de SOC (*Security Operation Center*), que traz visibilidade ininterrupta (24x7x365) das principais ameaças e eventos anômalos que estão ocorrendo na rede da empresa.

Outro exemplo de serviço gerenciado é o monitoramento contínuo de Gestão de Vulnerabilidades (GV) e Conformidades (GC), o qual por meio de um *vulnerability scanner* (Nessus, Qualys, Nexpose, entre outros) permite identificarmos as principais vulnerabilidades e itens de configurações seguras (*hardening*), respectivamente, precisam ser priorizados.

Realize uma avaliação da segurança de suas aplicações

Você sabe qual o grau de exposição a riscos de segurança de suas aplicações publicadas para a internet? Os ataques continuam e até mesmo se intensificam em momentos de crise. Aproveite para pedir ajuda especializada para uma avaliação de sua superfície de ataque.

A execução de um teste de invasão (*pentest*) em sua infraestrutura tecnológica e/ou a avaliação específica de uma *aplicação (web / mobile)* por meio de um EHT (*Ethical Hacking Test*) permitem mitigarmos riscos de acessos não autorizados e vazamento de informações, permitindo à empresa atuar de forma tempestiva na resposta dos riscos identificados.

Ative um serviço de inteligência de ameaças

A contratação de um SOC, a ativação de um serviço contínuo de gestão de vulnerabilidades e conformidades, bem como a execução de testes regulares de invasão, reduz mas não elimina riscos associados ao vazamento de informações, que neste momento poderiam ser utilizadas de forma ainda mais direcionada (*spear phishing*).

Neste sentido, serviços de monitoramento contínuo de ameaças *(Threat Intelligence*) procuram por dados da organização e/ou de seus funcionários que estejam sendo comercializados em redes *deep* e d*ark web* (mercado negro da internet).

7 Cibersegurança em tecnologia de automação

Raphael Gomes

Associate Partner
de Cibersegurança

São Paulo, Brasil

raphael.gomes@br.ey.com

www.linkedin.com/in/raphaelpereira

O cenário atual pode gerar um grande impacto na infraestrutura crítica do Brasil. A manutenção da operação é essencial para garantia da vida e muitas ações podem ser realizadas para contribuir com uma operação segura.

Listo abaixo alguns *insights* que podem ser utilizados para a continuidade das operações:

Shutdown ou redução da produção

- Em muitos casos, o *shutdown* não é possível por impactar a sociedade. Encontrar um caminho que garanta a continuidade dos serviços pode passar por uma avaliação de quais plantas e linhas de operação devem continuar e como manter esta operação íntegra. Vale a regra mais vale uma operando do que dez paradas.

Proteger a integridade dos funcionários

- O primeiro passo é criar medidas para proteger a equipe, buscando caminhos para evitar o contágio dos profissionais e perda de produtividade ou conhecimento;
- Aumentar o banco de currículos de profissionais habilitados nas tecnologias de OT acelera uma possível contratação temporária para substituir um funcionário afastado.

Foco

- Estabelecer o **foco** na garantia da disponibilidade da produção e dos serviços é essencial.

Fornecedores críticos

- Entrar em contato com os fornecedores críticos de OT e elaborar um plano de atuação em conjunto, incluindo a contratação pontual de horas ou profissionais adicionais para trabalho remoto e local em caso de emergências;
- Criar um método seguro de acesso remoto para o fornecedor criando mecanismos de controle de sua atuação através de gestão de mudanças ou dos mecanismos de SSO (*Single Sign-On*).

Operação "remota"

- A adoção de trabalho remoto, muitas vezes prejudicada pela segregação do ambiente, pode ser superada de forma segura com a adoção de controles no ambiente atual e a conexão do ambiente restrito a endereços IPs conhecidos e controlados;
- Para as ações de emergência, devem ser mantidas equipes locais, tomando-se sempre preocupações com a saúde e segurança das mesmas.

Suporte operacional

- Estabelecer uma conexão entre as equipes de TI e OT/TA é fundamental para estabelecer caminhos seguros para a implementação do acesso remoto, assim como construir mecanismos de suporte à operação.

Testes de segurança no acesso remoto e na conexão com a TI

- Realizar testes recorrentes de avaliação de riscos pela internet e acesso remoto pode ajudar a encontrar brechas na operação de contingência e criar soluções de contorno.

8 Pandemia de ameaças cibernéticas

Alex Aguiar
Sócio de Cibersegurança

São Paulo, Brasil

alex.aguiar@br.ey.com
www.linkedin.com/in/alex-aguiar

As ameaças de antes da pandemia e de agora não são tão diferentes em essência, e precisamos ter um olhar positivo sobre as crises. Mas os detalhes é que podem nos assombrar. Dessa forma, apresento abaixo uma visão de cinco ameaças que devem ser monitoradas dado o desenrolar da pandemia.

1. E-mails e páginas falsas (*phishing*)

As campanhas de *phishing*, com o envio de e-mails falsos com links e páginas falsas, certamente apelarão para a ansiedade da sociedade por mais informações acerca da Covid-19 não só na divulgação sobre notícias, como também no posicionamento do governo, entidades de saúde, palavras de especialistas etc.

Ou seja, interesse e oportunidade serão matéria-prima na tentativa de enganar as pessoas para obtenção de dados de usuários, roubo de senhas e outras informações confidenciais.

2. Malwares e aplicativos falsos

Você baixou aquele aplicativo para iOS e Android que mostra quais hospitais têm menos fila naquele momento? Instalou um aplicativo para acompanhar a evolução do novo coronavírus? Saiba que já foram relatados diversos aplicativos falsos se utilizando desse momento de pandemia.

3. Engenharia social

Com o aumento do trabalho em contingência e o *home office*, os colaboradores ficam ainda mais suscetíveis à engenharia social. Para muitos, o *home office* é realidade há muito tempo. Para outros, é algo totalmente novo. Então eduque as equipes, porque alguém pode ligar, dizer que é da TI, que a VPN tem de ser reinstalada e você sabe o fim da história.

Adicionalmente, estão aumentando os casos de recebimento de SMS falso (*smishing*) e ligações telefônicas de ONGs e entidades pedindo dinheiro para ajuda humanitária. Fiquem atentos para que sua ajuda alcance de fato quem precisa.

4. Vazamento de dados

Controlar dados já é uma tarefa hercúlea. Imagine agora a situação de um colaborador em quarentena por semanas. Em algum momento, vai bater a tentação de mandar um arquivo para o Gmail, por que não gravar aquele vídeo gigante no Google Drive... Afinal o meu Mac pessoal processará esse vídeo rapidinho.

A combinação de controles tecnológicos de segurança e a conscientização dos colaboradores são primordiais nesse tema.

5. O desconhecido

O desconhecido é o maior inimigo, tanto para os colaboradores **como** para a empresa, pois dele podemos esperar tudo e os recursos são finitos.

Usar este momento para refletir sobre o que pode dar errado e como se proteger contra o desconhecido é algo salutar para a empresa. E a forma mais cautelosa para se proteger do desconhecido é investir em inteligência. Ao menos você saberá que algo errado ocorreu e assim poderá reagir.

Onde encontrar mais informações

Portal de cibersegurança da EY Brasil

Clique aqui para acessar.

LGPD HUB

Clique aqui para acessar.

Pesquisa Global de Segurança da Informação da EY de 2020

Clique aqui para acessar.

Website EY Brasil

Clique aqui para acessar.

EY

Auditoria | Impostos | Transações Corporativas | Consultoria

Sobre a EY

A EY é líder global em serviços de Auditoria, Impostos, Transações Corporativas e Consultoria. Nossos insights e os serviços de qualidade que prestamos ajudam a criar confiança nos mercados de capitais e nas economias ao redor do mundo. Desenvolvemos líderes excepcionais que trabalham em equipe para cumprir nossos compromissos perante todas as partes interessadas. Com isso, desempenhamos papel fundamental na construção de um mundo de negócios melhor para nossas pessoas, nossos clientes e nossas comunidades.

No Brasil, a EY é a mais completa empresa de Auditoria, Impostos, Transações Corporativas e Consultoria, com 5.000 profissionais que dão suporte e atendimento a mais de 3.400 clientes de pequeno, médio e grande portes.

EY refere-se à organização global e pode referir-se também a uma ou mais firmas-membro da Ernst & Young Global Limited (EYG), cada uma das quais é uma entidade legal independente. A Ernst & Young Global Limited, companhia privada constituída no Reino Unido e limitada por garantia, não presta serviços a clientes. Para mais informações sobre nossa organização, visite ey.com.br.

ey.com.br
Facebook | EYBrasil
Instagram | eybrasil
Twitter | EY_Brasil
Linkedin | EY
Youtube | EYBrasil