



TENDÊNCIAS 2020

**A TECNOLOGIA ESTÁ SE
TORNANDO CADA VEZ
MAIS INTELIGENTE.
ESTAMOS PREPARADOS?**

ÍNDICE

Introdução

3 – 4

1

2020: A neblina se adensa

5 – 9

2

Machine Learning x Machine Learning: Criando segurança ou atacando?

10 – 13

3

Mudanças substanciais em termos de privacidade

14 – 17

4

De dispositivos IoT a edifícios e cidades inteligentes: “Smart is the new sexy”

18 – 22

5

Transformação digital e segurança da informação: o desafio para as empresas

23 – 26

Conclusão

27 – 28

INTRODUÇÃO

Considerando que os dispositivos são cada vez mais inteligentes, é inevitável questionar se os usuários também estão adquirindo “inteligência” suficiente para se beneficiar desses avanços tecnológicos sem sofrer contratempos.

Ano após ano, especialistas em segurança da ESET de todo o mundo se aventuram nos aspectos de segurança dos últimos avanços tecnológicos. E considerando que é inegável que os dispositivos estão se tornando cada vez mais inteligentes, surge uma pergunta: os usuários estão acompanhando os avanços tecnológicos em termos de “inteligência” necessária para aproveitá-los ao máximo sem sofrer contratempos? Ao longo dos cinco capítulos deste relatório, revisaremos diferentes aspectos relacionados à segurança, diferentes agentes sociais, como usuários, governos e empresas, e conceitos gerais, como privacidade, democracia, transformação digital e muito mais.

Tony Anscombe aborda o tema das eleições presidenciais dos Estados Unidos e os ecos das repercussões que as fake news e as denúncias de interferências estrangeiras tiveram em eleições anteriores. Infelizmente os Estados Unidos não tem sido o único lugar no mundo onde esse cenário ocorreu e, quase certamente, ao longo de 2020 será um tema que estará na agenda pública e política, então vale a pena rever como as (des) informações e as fake news podem desempenhar um papel nos processos democráticos que virão.

No capítulo “Machine Learning x Machine Learning: Criando segurança ou atacando?”, Jake Moore aborda este tema, que é um dos mais comentados dos últimos tempos. Esse termo tem sido usado para diferentes desenvolvimentos tecnológicos, mas em 2019 uma de suas aplicações ganhou relevância pública com a popularidade efêmera do FaceApp e com a melhoria das técnicas de deepfake que foram vistas ao longo do ano. Qual o impacto do Machine Learning na segurança? Poderia ser usado para atacar a segurança e a privacidade de usuários e organizações?

Todas estas questões estão intimamente relacionadas com a privacidade dos usuários. Lysa Myers, em seu capítulo, analisa como está a questão da privacidade depois do que aconteceu com a Cambridge Analytica, a implementação da legislação em diferentes níveis e as implicações para empresas e governos que terão o desencanto dos usuários em relação à privacidade de seus dados.

A tendência “Smart” não só atingiu os objetos que os usuários usam todos os dias, como já está tomando uma escala maior e podemos ver diferentes exemplos de edifícios inteligentes em todo o

mundo, e com a promessa de que em breve as cidades serão as próximas a juntar-se a este cenário. Será que isto pode causar novos tipos de ataques que misturam o digital e o físico? As condições de segurança existentes para que estas implementações se realizem sem colocar em risco os usuários/cidadãos e as organizações? Cecilia Pastorino desenvolve estas e outras questões em seu capítulo.

Essa mudança de paradigma talvez seja mais evidente nos processos de transformação digital que estão sendo executados em muitas empresas em todo o mundo, desafiando as equipes de TI a acompanhar o ritmo de todas as mudanças tecnológicas. Camilo Gutiérrez aprofunda esta questão e quais serão os desafios para o ambiente corporativo no futuro bem próximo.

Uma das ferramentas para poder estar preparado para o futuro é a informação. Por isso, leia este relatório de Tendências 2020 e saiba o que está por vir em 2020 e nos anos seguintes.



2020: A NEBLINA SE ADENSA

- Fake news
- Desinformação direcionada e propaganda
- O processo de votação?
- Des-mis-ti-fi-can-do tudo?



AUTOR

Tony Anscombe

Global Security Evangelist

2020: A neblina se adensa

O ano de 2020 pode ser outro ano confuso para o processo democrático. O que pode atrapalhar o nosso caminho na hora de tomar decisões baseadas em fatos?

Conforme avançamos rumo a 2020, há uma previsão de todo esse relatório de Tendências que é praticamente uma certeza: haverá reivindicações de interferência e manipulação nos processos eleitorais durante o ano.

Esses problemas são complexos e ainda que seja fácil apontar o dedo para a suspeita de interferência, pode ser difícil provar com uma certeza razoável. A complexidade começa devido a incidência de vários tipos de interferências que podem fazer com que os resultados eleitorais sejam liderados para um certo resultado ou para não representar realmente o voto emitido pelo eleitorado. Ao olhar para problemas cibernéticos ou on-line, eles oscilam entre notícias falsas e fraude nas urnas eleitorais, chegando a ter como alvo a parcela da população influenciável por informações tendenciosas.

As eleições presidenciais dos EUA de 2016 foram envoltas em controvérsias pós-eleição com reivindicações de notícias falsas, interferências de outros estados-nação e o potencial ataque do próprio processo de votação. Além disso, há reivindicações de que o referendo do Brexit no Reino Unido foi tendencioso devido a interferências e que, na América do Sul, a desinformação se espalhou pelo WhatsApp afetando possivelmente o resultado das eleições brasileiras. Como podemos esperar que os eleitores confiem no processo democrático quando tudo isso está encobrindo o desfecho?

Este capítulo resume alguns dos métodos que veremos ser usados indubitavelmente por indivíduos, grupos ativistas, estados-nação e até mesmo cibercriminosos em 2020 enquanto eles tentam interferir nos processos democráticos mundiais para seus próprios ganhos, quaisquer que sejam.



Fake news

O Collins Dictionary premiou esse termo como **Palavra do ano** em 2017. Sua ascensão à fama se deu principalmente devido às eleições presidenciais dos EUA de 2016 e às reivindicações contínuas dos candidatos de que artigos aparecendo na mídia e histórias se espalhando nas redes sociais não eram reais. O **significado do termo** é autoexplicativo e se refere ao sensacionalismo de informações falsas sendo disseminadas sob o pretexto de divulgação de notícias.

Às vésperas das eleições, Pew Research conduziu uma **pesquisa** referente a percepções sobre notícias falsas. O resultado foi impressionante, com 88% declarando que os norte-americanos estão muito ou um pouco confusos com os fatos básicos devido as fake news.

Ofcom, o regulador de mídia do Reino Unido, emitiu um **relatório** declarando que metade dos adultos do Reino Unido recebem notícias através de sites de mídias sociais, com 75% deles declarando que incluem o Facebook como fonte. E isso apesar da avaliação das mídias sociais ser percebida como não imparcial, confiável ou precisa. A TV permanece como a mais usada, com 75% dos adultos entrevistados listando-a dentre suas fontes de notícias, mas a influência das mídias sociais não deve ser subestimada e está aqui para ficar.

Há diferentes tipos de fake news: para lucros, para ganhos políticos, para crimes, boatos e brincadeiras virais. Os tipos podem até ser combinados: criar um boato que coloca um candidato político em maus lençóis pode criar um ganho político e, com a publicidade "certa" sendo exibida ao redor da história das notícias falsas, isso também pode gerar um ótimo lucro. Se os criadores de tal campanha puderem ser identificados, então é provável que tenham cometido um crime, mas identificar a fonte nem sempre é possível.

Na disputa para as eleições gerais do Reino Unido de 2019, uma organização de pesquisa, Future Advocacy, e um artista do Reino Unido, Bill Posters, criou um vídeo falso de mídias sociais ou o chamado "deepfake". O vídeo mostra os principais candidatos parecendo patrocinar um ao outro para primeiro-ministro. Esse exemplo de notícias falsas foi criado em uma tentativa de demonstrar a dificuldade em identificar o real do falso, e que a democracia está potencialmente sendo prejudicada.

Mas esse problema não é novo. Eu frequentemente fico no caixa do supermercado local e leio as principais notícias das capas das revistas: celebridades se separando, a família real britânica se divorciando ou alienígenas aterrisando no estacionamento. Espera-se que os leitores de tais revistas saibam que as histórias são falsas quando as comprem, mas quando pensamos em histórias da Internet que são divulgadas rapidamente para públicos muito maiores, não é tão fácil diferenciar o bom do ruim.

Algumas redes sociais e provedores de mecanismos de busca estão responsabilmente tentando combater o problema, sob pressão da revolta pública e política. Por exemplo, o Twitter anunciou recentemente o banimento de todas as propagandas políticas sobre candidatos, eleições e problemas importantes de política à frente das eleições presidenciais dos EUA de 2020. Mas esse é um tópico complexo e foi referido como violação da liberdade de expressão se é negada a habilidade a alguém de publicar ou colocar anúncios com um certo ponto de vista. Na realidade: conforme as notícias falsas se disseminam, as impressões da página aumentam e a receita dos anúncios é recebida, e nem todos os atores que exibem anúncios em websites são responsáveis.

O problema é a velocidade da disseminação da desinformação – uma história que apareça nas próximas horas irá se espalhar rapidamente, especialmente se o criador promovê-la e divulgá-la em múltiplas contas e redes ao mesmo tempo. As empresas responsáveis pelas plataformas inovaram os métodos de detecção e construíram mecanismos de relatórios para, quando possível, detectar automaticamente ou permitir que os usuários denunciem fake news. No entanto, confiar em relatórios é uma solução falível quando a desinformação já foi divulgada. Por isso, é provável que muitos usuários certamente não deem o próximo passo para denunciar e é improvável que aqueles que já viram (e talvez tenham sido influenciados) a desinformação se tornem cientes de sua retratação.

Como profissional de cibersegurança, considero notícias falsas que prejudicam a democracia como maliciosas – tanto quanto invasões de malware em seus dispositivos. Precisa haver uma solução tecnológica mais robusta para fazer com que as fake news parem de se propagar logo que aparecem e matá-las na fonte. Da mesma maneira que exploits zero-day são detectados por produtos antimalware. Com a adoção do machine learning, é provável que algumas soluções inovadoras apareçam no mercado que irão detectar e suprimir ou excluir ao menos algumas das fake news antes que o usuário se submeta a elas.

A educação também é uma solução de longo prazo para este problema, mas os resultados são mais lentos. Em julho de 2019, o governo do Reino Unido publicou um

novo guia de segurança para escolas e parte disso atualizou as condições da política de que toda criança irá aprender sobre tendência de confirmação e riscos on-line como parte obrigatória do currículo. Isso irá ajudar a habilitar os alunos a verem as técnicas usadas para persuasão e a identificar as fake news e os seus riscos, mas irá levar muitos anos para que toda uma geração possa entender o que pode ser real ou falso. (Meu colega Jake Moore irá trabalhar o espectro de deepfakes no capítulo Machine Learning x Machine Learning: Criando segurança ou atacando?) Entretanto, compreender o que é real ou falso dará à próxima geração confiança no sistema eleitoral democrático. Mais governos estão propensos a tomar essa postura proativa e adicionar isso as suas políticas educacionais. Se ainda não o fazem, deveriam.

Desinformação direcionada e propaganda

O abuso de dados pessoais da Cambridge Analytica chocou o mundo, mas não surpreendeu aqueles de nós que sempre diziam: "se você não está pagando por isso, então você é o produto"; por exemplo, cada usuário do Facebook nos EUA e Canadá [gera mais de US\\$ 130](#) para a empresa todo ano. O escândalo finalmente aconteceu quando três organizações de notícias combinaram recursos para causar tração suficiente para qualquer um perceber – após mais de dois anos.

Avançando um pouco na história, o Facebook foi multado em US\$ 5 bilhões pela Comissão de Comércio Federal dos EUA (FTC) por sua parte na violação dos dados. Não tenho certeza que realmente podemos descrever como uma violação, no entanto, já que documentos agora em domínio público mostram que o Facebook sabia o que estava acontecendo – foi mais um abuso de confiança para ganhos financeiros. No dia da multa do FTC foi anunciado que o valor de mercado do Facebook aumentou: estava claro que o mercado esperava que a penalidade fosse mais dura ou se entendeu que o acordo feito com a FTC foi na verdade a favor do Facebook.

A armamentização da informação, seja desinformação ou propaganda, está configurada para continuar e tomará muitos caminhos diferentes enquanto os benfeitores exploram e adoram novos métodos para atacar a demo-

cracia ou fazer dinheiro. No centro desse problema furtivo e invasivo está a mineração de dados, algo que não podemos ver e que para muitas pessoas é difícil de entender. Os pontos de dados disponíveis sobre indivíduos, dado que a maioria das pessoas [compartilha excessivamente nas mídias sociais](#), são extensos. A habilidade de ajustar e manipular a mensagem enviada para um indivíduo é orientada pela tecnologia, desbloqueando o poder para individualizar as mensagens enviadas para milhões de pessoas, tudo com o clique de um mouse.

O processo de votação?

Este também não é um problema novo e se relaciona a ambos, sistemas de votação eletrônico e em papel. Além disso, é um problema improvável de ser resolvido num futuro próximo.

Muitos estados nos Estados Unidos gastaram milhares de dólares para atualizar os sistemas que serão usados nas eleições de 2020. Um estado, a Pensilvânia, beneficiou-se de [US\\$ 14 milhões para otimizar seus sistemas eleitorais](#), mas mesmo os novos sistemas podem ser vulneráveis devido ao sistema operacional subjacente, o Windows 7, o qual – a menos que uma taxa seja paga – não irá mais receber patches da Microsoft assim que esta versão do sistema operacional atingir seu “fim da vida” em janeiro de 2020, 11 meses antes das eleições presidenciais de 2020 dos EUA.

Na conferência de *hacking* DEF CON número 27, realizada em agosto de 2019, houveram desafios em tempo real para [encontrar falhas em sistemas eleitorais](#). Um de tais experimentos mostrou vulnerabilidades em um sistema de impressão de voto. Neste exemplo, o atacante tinha acesso físico irrestrito e conexão direta com os dispositivos, o que nunca deveria acontecer no mundo real. Espero que alguém possa perceber um atacante desmontando um terminal e conectando fios a ele. No entanto, isso depende dos dispositivos serem fisicamente protegidos antes e durante o processo de votação, o que não foi o caso em alguns exemplos em eleições anteriores. Isso também pode perder a relevância se os dispositivos permanecerem independentes e nunca estiverem conectados a uma rede pública. Enquanto há muitos disposi-

tivos que teoricamente poderiam estar vulneráveis, isso não significa necessariamente que eles podem ou serão explorados.

Está claro que soluções tecnológicas para ambos, cadastro e votação continuarão a ter problemas. Continuamos a testemunhar brechas de dados em massa e comprometimento de sistemas em empresas e departamentos governamentais, então por que a tecnologia ou processos de votação estariam isentos de ataques similares? A boa notícia é que as eleições presidenciais dos EUA de 2016 elevaram o alerta de vulnerabilidades possíveis no sistema eleitoral sendo usado, o que resultou diretamente em atribuição de orçamento e compreensão da necessidade dos sistemas estarem protegidos por design.

Des-mis-ti-fi-can-do tudo?

Para 2020, certamente haverá muitas eleições ao redor do mundo e incontáveis problemas destacados em seus sistemas e processos, ambos tecnológicos e físicos. O uso de todos os métodos mencionados aqui é esperado, mas a questão é: em que escala serão usados e se a interferência mudará o resultado?

Como eleitores e, esperançosamente, adeptos da democracia, iremos pressionar as empresas que distribuem fake news e desinformação para que sejam detectadas e parem com a prática. No entanto, altos lucros para permitir essas práticas e falta de engajamento dos consumidores, significa provavelmente que iremos continuar a ver o fluxo da má-informação, seja levemente desinformativa ou fabulosamente fabricada, continuar fluindo.

Como acontece com muitas práticas questionáveis, como o abuso da privacidade do consumidor a que estivemos sujeitos pelos últimos 10 anos, sem intervenção governamental e regulamentação ou legislação, iremos prosseguir até um ponto onde essa prática não poderá mais ser tolerada. No entanto, não espere que isso aconteça nos próximos 12 meses.

MACHINE LEARNING X MACHINE LEARNING: CRIANDO SEGURANÇA OU ATACANDO?

- Enganando olhos desatentos
- Enganando o algoritmo
- Uma explosão ou uma expulsão?



AUTOR

Jake Moore
Security Specialist

Machine Learning x Machine Learning: criando segurança ou atacando?

Os avanços em machine learning trouxeram benefícios consideráveis para os defensores da cibersegurança, mas o potencial da tecnologia não está perdido para aqueles que estão buscando agregá-lo para fins inescrupulosos.

O *Machine learning* (ML) está, sem dúvida, mudando nossas vidas. Poder computacional aumentado e o uso de vastos armazéns de dados estão rapidamente melhorando nossas capacidades em múltiplas indústrias. Além disso, se o primo distante do ML também conhecido como verdadeira Inteligência Artificial (AI) decolar também e computadores começarem a “pensar por si mesmos”, estaremos em um maravilhoso futuro onde muito do que outrora se imaginava ser impensável pode se tornar possível. Por agora, no entanto, a AI autossustentável parece muito distante – enquanto o ML está avançando em um dos desenvolvimentos tecnológicos mais animadores da história.

O ML também trouxe vários [benefícios para os ciberdefensores](#), incluindo escaneamento eficiente, detecção mais rápida e melhorias na habilidade de detecção de anomalias. De fato, algumas empresas de cibersegurança vêm tirando vantagem da tecnologia por anos para melhorar as capacidades de detecção de seus produtos.

No entanto, e se o ML for usado indevidamente para nos atacar e aos sistemas que construímos? Não é difícil de ver porque e como o ML- ou mesmo malware baseado em AI pode oferecer vetores novos e únicos de ataque – mais poderosos do que os que estamos acostumados atualmente. Então, está se tornando claro que o ML será um componente importante na batalha futura.

A tecnologia vem avançando muito rapidamente em outros aplicativos também. Neste capítulo de Tendências, iremos explicar tudo sobre duas maneiras que os algoritmos de ML poderiam ser armados para causar problemas.



Enganando olhos desatentos

Certamente, você viu um dos muitos vídeos convincentes de troca de rostos que aparecem, especialmente em mídias sociais. Tais deepfakes – vídeos, áudios ou imagens manipuladas que foram projetados para replicar a aparência e som de humanos reais – podem ser desconcertantemente legítimos e até chocantes. As deepfakes podem até envolver celebridades ou figuras públicas aparentemente envolvidas em comportamento inesperto ou em dizer algo ultrajante e que não seria normalmente apoiado por elas.

As deepfakes estão aumentando de qualidade a uma velocidade impressionante, como visto em vídeos como [este aqui](#) onde fazem um Barack Obama criado por computador dizer algo que o verdadeiro não disse na verdade. Além do mais, quando você observa um [Bill Hader](#) sendo transformado sem esforço entre Tom Cruise e Seth Rogan, faz você perceber que podemos realmente ter um grande problema em nossas mãos a menos que essa ameaça seja abordada. Como com tudo na Internet, o futuro poderia levar a esta tecnologia ser usada para prejudicar figuras públicas fazendo com que elas parecessem dizer o que seus criadores quisessem, para prejudicar a sociedade ou mesmo para manipular eleições ao redor do mundo.

Estamos preparados para o impacto real das deepfakes? Com escândalos políticos, pseudonudes e cenários quase inimagináveis envolvendo vídeos falsos, podemos estar olhando fixamente sem entender para o começo de uma epidemia onde a linha entre a verdade e a mentira pode se tornar impossível de determinar. Quais impactos sociais as deepfakes poderiam ter na sociedade? À luz de todo o escândalo Cambridge Analytica, no qual cientistas de dados foram capazes de transformar pesquisas e dados gráficos sociais do Facebook em uma arma de mensagem política através de caracterização psicográfica, parece que as deepfakes poderiam acelerar tais transformações ao influenciar o público nas eleições. Será que chegaremos a um ponto onde não confiaremos em nossos próprios olhos e ouvidos?

Após o FaceApp ter sido literalmente colocado sobre nossos rostos e após acabarem os gemidos e risos, surgiu uma questão a respeito da qualidade de tal “feitiçaria” –

será que o aplicativo poderia um dia criar vídeos das pessoas sem seu conhecimento? Você precisa de muitos dados (muitas fotos, vídeos e gravações de voz) mesmo para fazer um clipe deepfake curto onde o criador está no controle do que é dito. No entanto, obter uma quantidade significativa de dados sobre uma figura não pública é uma tarefa difícil por si só. Mas isso é apenas pensando com a mentalidade de 2019; e se pensarmos no próximo ano ou em uma década? Seria necessário apenas um ou duas histórias curtas do Instagram para que alguém produzisse uma deepfake que a maioria dos seus amigos on-line acreditaria? Prevejo que isso é o que irá acontecer e haverá um aplicativo em nossos telefones que irá criar tais deepfakes naturalmente e sem esforço.

Ao longo da próxima década, veremos alguns vídeos falsos inimagináveis anteriormente aparecendo com figuras públicas, mas em breve eles irão incluir pessoas mais próximas, como nossos colegas, nossos pares, nossos membros familiares. Não há dúvidas de que os sites pornográficos irão explorar celebridades de maneiras obscuras, mas, muito mais, os cibercriminosos irão definitivamente usar tal tecnologia com grande sucesso para caçar vítimas. As deepfakes poderiam muito facilmente turvar a água entre fato e ficção, o que por sua vez poderia fazer com que alguns de nós não confiemos em mais nada – mesmo quando apresentadas com o que nossos sentidos nos dizem para acreditar.

Então o que pode ser feito para nos preparar para essa ameaça? Primeiro, precisamos educar melhor as pessoas sobre a existência de deepfakes. As pessoas precisam aprender a tratar até os vídeos mais realistas que veem com traços de ceticismo. Além disso, ainda que difícil, a tecnologia precisa desenvolver uma melhor detecção de deepfakes. Ainda que o ML esteja no coração da criação delas em primeiro lugar, precisa haver algo no lugar que aja como o antídoto, ser capaz de detectá-las sem confiar somente na intuição humana. Além disso, plataformas de mídia social precisam reconhecer e abordar a ameaça potencial o mais cedo possível já que é aí que os vídeos deepfake tem maior capacidade de disseminação e têm um impacto prejudicial na sociedade.

Enganando o algoritmo

O **reconhecimento facial** está se tornando mais prevalente na tecnologia atual. A implementação do reconhecimento facial pode ainda não ter uma precisão de 100%, mas, novamente, ainda é apenas 2019 e as coisas tendem a apenas melhorar, certo?

Algumas cidades nos Estados Unidos baniram o reconhecimento facial sendo usado para cumprimento da lei após ele ter identificado erroneamente 26 pessoas cidadãs cumpridoras da lei como criminosas. Na verdade, uma **pesquisa** do Escritório de Prestação de Contas Governamental dos EUA descobriu que os algoritmos do FBI eram imprecisos em 14% das vezes, além de serem mais prováveis de errar a identificação de pessoas segundo suas etnias e mulheres. Além disso, a Microsoft recentemente **recusou-se a instalar tecnologia de reconhecimento facial** para uma força policial dos Estados Unidos devido à preocupação com a tendência de ML. É aqui que os dados são inseridos por humanos, que tendem a ter uma variedade de tendências não intencionais que influenciam o resultado do ML.

No entanto, há argumentos para que o reconhecimento facial seja executado em todos os lugares e instalado com as milhões de câmeras de vigilância que já capturam quase todos os nossos movimentos em público. Por exemplo, se você pegar o reconhecimento facial em sua forma básica fundamental, ele oferece uma forma de coletar informações sobre quem esteve onde e a que horas. Isso não está muito longe de um bom policial que pode reconhecer o criminoso local em seu caminho (conheço alguns policiais que podem fazer isso – eles têm memórias fantásticas). Portanto, se com o tempo o reconhecimento facial se tornar próximo de 100% de precisão, então ele poderá vigiar todos os nossos movimentos.

Mas se o cumprimento da lei sabe o paradeiro de criminosos e suspeitos conhecidos, e os criminosos que usam software em sua vantagem ou roubam grandes bases de dados de dados de localização confidenciais? Poderia ser possível que as bases de dados dos rostos das pessoas poderiam estar comprometidas, o que significa que técnicas de verificação como reconhecimento facial ou de voz poderiam ser enganadas e, portanto a segurança multicamadas poderia ser transpassada.

Uma explosão ou uma expulsão?

Ataques completos e poderosos de ML estão vindo e não vamos esquecer que alguns ataques são atualmente insondáveis devido à escala de poder que usam, então eles têm o potencial de ser maiores do que podemos antecipar. É possível que o ML possa ser munido pelos atacantes, então precisamos nos preparar para tais ataques e estar cientes de como combatê-los. Ataques direcionados ao ML poderão ser capazes de aprender o que funcionou e o que não funcionou rapidamente, retreinando a si mesmos para conseguir ultrapassar defesas existentes. Os defensores de segurança de computador precisam entender como esses ataques movidos por ML serão criados, quais poderão ser suas capacidades e unir-se para enfrentar esses futuros ciberataques.

MUDANÇAS SUBSTÂNCIAIS EM TERMOS DE PRIVACIDADE

- Design para privacidade e segurança
- Melhoria da tecnologia de anúncios
- Consequências legislativas para violações da confiança
- Melhoria da autenticação e verificação
- Vamos mudar o rumo dessa embarcação



AUTORA

Lysa Myers

ESET Senior Security
Researcher

Mudanças substanciais em termos de privacidade

A confiança em nosso ambiente digital compartilhado não tem tido um bom andamento ultimamente, e mais e mais pessoas estão no limite sobre proteger seus dados digitais. O que tem sido feito e, ainda mais importante, o que resta a ser feito para que a maré mude?

Há um certo “rito de passagem” que acontece quando você fala sobre segurança e privacidade por um tempo: você faz previsões de como serão as ameaças no futuro, e terá passado tempo suficiente para que você possa verificar a precisão de suas previsões.

Isso tudo acontece principalmente em uma escala de um futuro próximo, como esse próprio capítulo de Tendências. Algumas vezes está numa escala de uma década ou mais. Em minha própria experiência com este fenômeno, percebi alguns temas, a maioria dos quais se passa ao redor de ganhar ou perder confiança em nosso ambiente on-line compartilhado.

Enquanto eu decidia o que escrever para este capítulo, fiz uma pesquisa na Internet pela frase “ano da privacidade” e adicionei um ano recente, por exemplo, “ano da privacidade 2018”. As manchetes incluindo esta frase podem ser um bom indicador de que o autor pensou que uma grande mudança estava por vir em relação à percepção pública da privacidade, seja positiva ou negativa. Acho que a primeira vez que declarei isso sobre um ano em análise foi em 2013, então fiquei curioso para saber quantas vezes isso tinha sido declarado. Para cada ano de 2009 a 2015, aqueles termos de pesquisa retornaram mais de um milhão de resultados. Após isso, cada ano retornou “apenas” de oitocentos a novecentos mil resultados.

Isso significa que 2016 foi o ano que muitas pessoas coletivamente abandonaram todas as esperanças de terem controle sobre suas informações pessoais? De algumas maneiras, pode ser o caso; parece haver um certo senso de resignação coletiva. Mas também parece que atingimos um ponto onde legisladores e juizes começaram a acompanhar a ira coletiva provocada por uma barreira constante de gafes e violações de privacidade.

E essa barreira continuou – somente em 2019, vimos al-

guns poucos [países](#) e estados norte-americanos [aprovar ou implementarem leis novas ou expandidas de violação](#). Também vimos [vários estados dos EUA](#) impulsionarem a legislação da privacidade de dados (ainda que apenas na Califórnia essa legislação tenha sido aprovada). Várias multas consideráveis foram impostas em empresas responsáveis por [violações de dados recentes](#) (ainda que essas sejam geralmente consideradas como meros tapas no pulso). Executivos de [empresas invadidas](#) tiveram que testemunhar diante de audiências no congresso sobre esses incidentes.

A mudança tem sido lenta e, discutivelmente esses esforços não tiveram uma diferença positiva ainda. O consenso geral entre boa parte da população norte-americana é que eles sentem que [não podem confiar](#) nas empresas para proteger seus dados e isso também ocorre em [outros países](#). Essa situação, junto à fraude crescente e outros tráfegos malignos, criou um [ambiente de “baixa confiança”](#) no qual estamos cada vez mais interconectados, mas nos sentimos cada vez mais inseguros. Quando temos que abordar tudo na Internet com paranoia e ceticismo, as pessoas se sentem compreensivelmente relutantes em se comprometer com ela.

Em segurança, frequentemente dizemos que é uma boa prática “confiar, mas verificar”: na situação na qual nos encontramos agora, a desconfiança é crescente e os métodos de verificação estão cheios de buracos. Até solucionarmos isso, a Internet continuará a ser um lugar assustador para a maioria das pessoas.

Então o que precisamos fazer para sair dessa sensação onipresente de desconfiança?

Design para privacidade e segurança

Uma das coisas mais importantes que precisa ser feita para melhorar a confiança do consumidor é criar produtos e serviços de tecnologia que sejam projetados tendo segurança e privacidade em mente desde o início. A Associação Internacional de Profissionais de Privacidade (IAPP) criou um documento delineando suas recomendações para os princípios da [Privacidade por Design](#).

Muitas das coisas mencionadas nesta publicação são o que se pode esperar: ganhar confiança através da abertura e transparência, decretar segurança de ponta a ponta, criar políticas que estabelecem responsabilidade para o negócio e obter consentimento informado e contínuo dos clientes. Mas há mais uma recomendação particularmente notável e que muitas pessoas podem achar surpreendente: permitir funcionalidade completa enquanto se respeita a privacidade, de tal maneira que beneficie a ambos, a empresa e o usuário.

Por conta do modelo atual de muitos locais da Internet usarem os dados do consumidor como um produto a ser vendido, essa recomendação particular pode precisar de um pensamento verdadeiramente inovador, “fora da caixa”. Empresas que conseguem realizar esse feito estão propensas a ter uma vantagem significativa no mercado.

Melhoria da tecnologia de anúncios

Já que estamos falando da venda de dados do consumidor, também deveríamos discutir melhorias necessárias na tecnologia de anúncios. Em [uma pesquisa](#), menos de 20% dos entrevistados acharam que os anúncios direcionados tinham comportamento ético. Em [outras pesquisas](#), descobriu-se que em alguns casos anúncios direcionados poderiam na verdade se tornar um contra-ataque e causar menor interação com o consumidor.

Empresas que usam táticas de vendas de alta pressão como [escassez e testemunho social](#) também não evoluem muito bem. Uma pesquisa no Reino Unido relatou que quase metade dos entrevistados disse que esse comportamento faria com que eles desconfiassem da empresa. Um terço expressou uma reação emocional negativa (como aversão ou desprezo) e 40% relatou que essas táticas fariam com que eles fizesse o oposto de qualquer ação que fosse sugerida.

Quanto maior a frequência que somos bombardeados com táticas de vendas de alta pressão e táticas de vigilância assustadoras, mais rapidamente declina sua (muito limitada) eficácia. Dado que muitos profissionais de marketing fizeram uso excessivo dessas estratégias, é provável que elas tenham sido oportunidades limitadas para outras empresas. Precisamos de formas mais eficazes de marketing que sejam honestos, transparentes e respeitosos com os nossos consumidores.

Consequências legislativas para violações da confiança

Não é provável que o sentimento público sobre a credibilidade das empresas de tecnologia vá melhorar até que seja mais provável que elas possam perder ao menos tanto quanto seus consumidores perdem quando incidentes de privacidade ocorrem. Ainda que multas recentes por violação de privacidade nos EUA e Reino Unido estejam quebrando recordes, elas representam uma pequena gota no balde relativo aos rendimentos que grandes empresas fazem com nossos dados. Até que essas multas se aproximem de valores que incluam um maior percentual do rendimento de uma empresa, elas continuarão a ser mais um impedimento para empresas pequenas do que para megacorporações.

Melhoria da autenticação e verificação

Nomes de usuários e senhas simplesmente não são mais suficiente para manter as identidades das pessoas seguras. Isso pode diminuir a confiança para ambos, portadores de contas on-line e das pessoas interagindo com contas potencialmente sequestradas. A autenticação multifatorial melhora significativamente essa situação, mas poucas pessoas a adotaram. Para mudar isso, precisaremos de educação melhorada sobre esta tecnologia, mais empresas oferecendo incentivos para usá-la, além de melhorias continuadas em sua usabilidade.

Vamos mudar o rumo dessa embarcação

Pediram-me pela primeira vez para predizer o estado da segurança na Internet há uma década, portanto, um pouco mais de uma década atrás. Eu disse que conseguia ver as coisas caminhando por um dos dois caminhos: ou ficaríamos mais sábios coletivamente e as coisas estariam bem, ou continuaríamos a meter os pés pelas mãos e a Internet seria um "aterro de entulho inutilizável". Ainda que ninguém iria argumentar com sucesso de que as pessoas estão usando a Internet menos do que usavam há dez anos, também tivemos que passar por muito mais lixo de Internet agora do que tínhamos que passar nos anos 2000.

Aqueles dentre nós que vem trabalhando em cibersegurança há mais tempo, desde o começo da indústria, tem vivido esse estado de desconfiança por décadas; vimos a Internet ser construída sob estruturas instáveis que fizeram pouco (se fizeram) para prevenir o mau uso. Felizmente, também estivemos pensando – e falando – sobre o que precisa ser feito para solucionar isso. Não é muito tarde para fazer movimentos significativos para apontar os esforços de privacidade de volta para a direção certa. É minha esperança que a vontade para as mudanças necessárias continue a crescer, para que possamos fazer essas mudanças antes que minha próxima década neste ramo tenha passado.



DE DISPOSITIVOS IOT A EDIFÍCIOS E CIDADES INTELIGENTES: “SMART IS THE NEW SEXY”

- Edifícios Inteligentes
- Cidades inteligentes
- Ataques a infraestruturas inteligentes
- Malware
- Roubo de identidade
- Roubo de informações críticas



AUTORA

Cecilia Pastorino

Security Researcher

De dispositivos IoT a edifícios e cidades inteligentes: "smart is the new sexy"

À medida que mais e mais cidades incorporam tecnologia inteligente que muda a forma como os municípios gerenciam suas operações e serviços básicos, qual é o impacto desses desenvolvimentos do ponto de vista da segurança?

Desde 1994, com o aparecimento do primeiro telefone inteligente, esta palavra tem sido usada nos anos seguintes para definir qualquer dispositivo que melhore as suas funções através de um software e uma conexão à Internet. Em 2009, Kevin Ashton, co-fundador do Auto-ID Center do MIT, usou pela primeira vez a expressão Internet of Things (IoT) publicamente e, desde então, o crescimento e a expectativa em torno do termo cresceram exponencialmente.

A década de 2010 é caracterizada pela revolução da Internet das coisas com o aparecimento de relógios, termostatos, luzes, fechaduras, câmeras, brinquedos, geladeiras e todos os tipos de dispositivos inteligentes que alguém pode imaginar e depois se tornar parte de casas, escritórios, edifícios e até mesmo cidades inteligentes.

Hoje em dia, o potencial da Internet das coisas não está apenas na automação de tarefas, mas também no processo analítico que pode ser realizado a partir dos grandes volumes de informação gerados. As estruturas inteligentes aproveitam uma variedade de tecnologias interdependentes, como a inteligência artificial (IA), as redes sem fios de banda larga, a computação em nuvem, os sensores e os dispositivos IoT. A grande quantidade de informação gerada por sensores e dispositivos de rede é armazenada em grandes bases de dados e processada por tecnologias de inteligência artificial e análise de dados para melhorar a eficiência operacional e promover um ambiente seguro e produtivo. Estas características são o que levam estes sistemas a serem chamados de inteligentes. No entanto, dado que a inteligência nem sempre significa segurança e que a tecnologia avança a passos largos, alguns de nós podemos nos perguntar quando é que a segurança irá finalmente acompanhar estes avanços a partir do design.

Edifícios Inteligentes

Os edifícios inteligentes usam a tecnologia para controlar diferentes variáveis que fazem parte do ambiente, a fim de proporcionar maior conforto, contribuir para a saúde e a produtividade daqueles que trabalham ou vivem neles. Para fazer isso, os edifícios usam o que é conhecido como Building Automation Systems (BAS). A partir de dispositivos IoT, como sensores de iluminação e/ou temperatura, câmeras, controles de acesso etc., essas construções são capazes de analisar, prever, diagnosticar e manter diferentes ambientes, além de automatizar processos e monitoramento em tempo real. Alguns exemplos são temperatura ambiente, iluminação, sistema de câmeras de segurança, elevadores, estacionamento, abastecimento de água, entre muitos outros.

As vantagens da implementação de dispositivos inteligentes são amplas. Por exemplo, como Tony Anscombe [explicou](#) em uma conferência na qual abordou a questão da segurança em edifícios inteligentes, um renomado hotel na cidade de Las Vegas implantou um sistema de automação para o ar-condicionado que só ligava a refrigeração quando havia hóspedes. Essa decisão representou no primeiro ano de instalação do sistema inteligente uma economia de aproximadamente dois milhões de dólares, graças à economia de energia que significou a automação desse processo. Por outro lado, um supermercado no Reino Unido [instalou](#) em seu estacionamento um sistema inteligente que aproveita a circulação de carros para gerar energia, que é usada para abastecer suas caixas registradoras.

Cidades inteligentes

Na edição de 2019 da "[Consumer Electronics Show](#)", foram apresentadas diferentes iniciativas de cidades inteligentes que estão sendo implementadas (ou planejadas) em todo o mundo. Algumas dedicadas a melhorar o transporte através de sensores que avaliam o fluxo de tráfego e, com base nessas medições, gerenciam o controle de semáforos. Outras enfocadas em automatizar a iluminação com base em sensores de luz, medir a temperatura, adicionar sistemas de monitoramento através de redes de câmeras e muitos outros sensores para coletar informações que serão analisadas em uma central para saber tudo o que ocorre na cidade. Como em edifícios inteligentes, mas em larga escala, com base nas informações coletadas de sensores e dispositivos, o aprendizado de máquina é usado para analisar esses dados e automatizar os serviços com eficiência.

O problema é que muitas dessas cidades apenas estão preparadas para gerenciar com segurança os grandes volumes de informações que esses sistemas implicam e que um invasor pode facilmente acessar os sensores, modificar medições e alterar serviços de transporte, tráfego, iluminação ou outros serviços de infraestrutura críticas. Já vimos provas de conceito de diferentes ataques a cidades inteligentes e [sistemas automatizados](#) em conferências internacionais como [Black Hat](#) ou Defcon; portanto, a qualquer momento, esses exemplos em ambientes controlados podem se tornar realidade. Além disso, se cidades como Atlanta, nos Estados Unidos, cujo projeto é [se tornar uma cidade inteligente líder em todo o mundo](#), não souberam evitar ameaças existentes, como o [ransomware](#), por que acreditar que estão preparadas para enfrentar maiores desafios? De fato, na conferência Smart City Expo realizada em setembro de 2019 na mesma cidade, especialistas expressaram preocupação de que o [rápido crescimento de cidades inteligentes não esteja sendo acompanhado pela capacidade de torná-las seguras](#), portanto que é necessário reavaliar a maneira de abordar a segurança para esse tipo de cidade.

Ataques a infraestruturas inteligentes

Embora pareça que ataques a prédios ou cidades inteligentes só podem ser realizados por meio de planos direcionados e elaborados nos quais os cibercriminosos apontam para um alvo específico, a verdade é que muitos Building Automation Systems (BAS), bem como sensores e dispositivos de cidades inteligentes, são expostos diretamente à Internet. Atualmente, mais de 35.000 sistemas BAS e centenas de milhares de outros dispositivos críticos disponíveis na Internet em todo o mundo podem ser encontrados em mecanismos de pesquisa como Shodan ou Cencys.

Muitos desses dispositivos ou sistemas não possuem uma autenticação ou proteção suficientemente fortes contra ataques de força bruta, não são atualizados, não são protegidos por soluções de segurança ou simplesmente possuem configurações inseguras que podem permitir que um invasor assuma o controle do dispositivo.

Malware

Apesar dos sistemas inteligentes de cidades ou edifícios não navegarem na web e não abrirem e-mails, ainda assim devem estar protegidos contra qualquer malware que possa dar aos cibercriminosos acesso a informações críticas ou causar problemas ao computador.

A propagação de códigos maliciosos pode ocorrer através de portas expostas à Internet, vulnerabilidades nos sistemas ou mesmo através do acesso físico a portas USB desprotegidas ou ao alcance de qualquer transeunte. A proteção da rede também não deve ser negligenciada, especialmente aquela na qual serão conectados dispositivos pessoais de usuários que possam estar comprometidos.

Entre os vários códigos maliciosos que podem atacar os sistemas de computadores de prédios ou cidades inteligentes, podemos destacar aqueles que usam uma botnet como ferramenta, especialmente considerando casos recentes de botnets direcionadas a dispositivos IoT, como uma [nova variante da botnet Mirai](#) ou o último [ataque aos computadores Mikrotik](#) com o objetivo de minerar criptomoedas. Será que, em um futuro não muito distante, os dispositivos IoT de uma cidade inteira poderão ser usados por um invasor para mineração de criptomoedas? Sem dúvida, o [criptojacking](#) é uma das ameaças que podem afetar as infraestruturas inteligentes, especialmente considerando o grande poder de processamento que caracteriza esses computadores, mas não é a única.

Há três anos, em nosso artigo sobre as [Tendências de 2017](#), apresentamos o conceito de "Jackware" para descrever software malicioso que tenta controlar um dispositivo cujo objetivo principal não é o processamento de dados ou a comunicação digital. O conceito de "Ransomware of things" é imediatamente aparente e se refere ao malware capaz de bloquear o acesso a dispositivos inteligentes. Nesse ano, discutimos uma prova de conceito que envolvia um carro em que o usuário recebeu uma mensagem em seu telefone indicando que ele tinha que pagar uma quantidade de criptomoedas para recuperar o controle de seu veículo. Talvez possamos extrapolar esse conceito para edifícios inteligentes ou sistemas de controle nas grandes cidades?

O que aconteceria se um atacante conseguisse comprometer o sistema de automação de um edifício inteligente e, em seguida, ameaçar assumir o controle em troca do pagamento de um resgate de vários milhares de dólares? A verdade é que já foram [relatados incidentes desse estilo](#) em que edifícios completos foram comprometidos.

Roubo de identidade

O controle do acesso a edifícios inteligentes geralmente ocorre por meio de sistemas computadorizados nos quais o usuário se identifica com dados biométricos ou cartões magnéticos. Esses sistemas podem ser atacados através de Engenharia Social ou falhas na implementação, o que permitiria a um usuário não autorizado obter acesso físico a setores restritos.

Por outro lado, a representação da identidade digital por um atacante pode causar estragos, caso consiga obter privilégios de administrador que lhe permitam controlar o sistema livremente. Muitas vezes, isso ocorre através de ataques de Engenharia Social nos quais o atacante consegue se apossar dos dados de login e do acesso da vítima, que são usados para instalar códigos maliciosos, roubar informações, mover-se no sistema ou várias outras formas de ataques.

Roubo de informações críticas

Os bancos de dados são um alvo atrativo para os cibercriminosos, especialmente quando contam com informações valiosas que podem ser vendidas ou dados de login que lhes permitem um movimento lateral. Se adicionarmos a isso a grande quantidade de informações armazenadas nos sistemas de análise de big data e inteligência artificial encontradas em prédios e cidades inteligentes, esses bancos de dados se tornam um alvo de interesse para os cibercriminosos e grupos de ciberespionagem.

Por outro lado, os sensores e dispositivos de IoT usados na maioria dos edifícios e infraestruturas inteligentes também podem ser um ponto de entrada para a rede, o que permitiria que um cibercriminoso tivesse maiores

privilégios ou fizesse movimentos laterais dentro da infraestrutura. É o caso de um cassino que foi vítima de um ataque no qual cibercriminosos entraram em sua rede depois de tirar proveito de uma [vulnerabilidade no termostato inteligente de um aquário](#) localizado no saguão. Eles conseguiram se infiltrar na rede e acessar o banco de dados do cassino, roubando informações que incluíam os dados pessoais dos apostadores.

Após essa análise, podemos dizer que edifícios e cidades inteligentes não são mais uma previsão de ficção científica, mas são uma realidade que está entre nós; e embora os incidentes de segurança relatados ainda possam ser considerados casos isolados, ataques contra a construção de sistemas de controle ou cidades já estão entre os alvos dos cibercriminosos.

As medidas e considerações de segurança para lidar com essas novas ameaças são as mesmas que reiteramos antes de cada nova evolução tecnológica: reservar um orçamento de acordo com a segurança, contar com programas de gerenciamento de vulnerabilidades, manter os sistemas atualizados, monitorar a rede e dispositivos e contar com ferramentas de segurança e parceiros que tenham conhecimentos no campo da segurança.

Projetos de construção que incluem a implementação de cada vez mais soluções tecnológicas estão crescendo, incorporando todos os tipos de dispositivos para torná-los mais "inteligentes", mas essas medidas de segurança são consideradas dentro dessa inteligência?

Por outro lado, o apoio à legislação que regulamenta a segurança desde o projeto de dispositivos inteligentes é extremamente necessário e é algo que provavelmente surgirá nos próximos anos, principalmente após as novas [iniciativas do Reino Unido](#) e do estado da [Califórnia](#) nessa área. Assim como existem padrões que regulam dispositivos críticos, é hora de começar a analisar quais são as regras e medidas de segurança que devem ser cumpridas pelos dispositivos inteligentes que interagem com nossas informações e privacidade.

A maioria das cidades do mundo já possui câmeras e sensores conectados à Internet que coletam e enviam permanentemente informações para executar diferentes

serviços. Muitos de nós já moramos nessas cidades e, em um futuro não muito distante, passaremos grande parte de nossa jornada de trabalho vivendo ou fazendo compras em edifícios hiperconectados, cheios de tecnologia. E embora todos esses avanços possam ser emocionantes e cativantes, não devemos esquecer que, por trás de tudo isso, deve haver, acima de tudo, pessoas inteligentes.



TRANSFORMAÇÃO DIGITAL E SEGURANÇA DA INFORMAÇÃO: O DESAFIO PARA AS EMPRESAS

- Mudanças em TI devem significar mudanças no gerenciamento da segurança
- Variedade de tecnologias como mecanismo de mudança
- O caminho da mobilidade
- Conceitos que devem ser mantidos na transformação digital
- Então, o que fazer nas empresas?



AUTOR

Camilo Gutiérrez

ESET Senior Security
Researcher

Transformação digital e segurança da informação: o desafio para as empresas

À medida que as organizações decidem embarcar ou continuar no caminho da transformação, elas precisam repensar todos os aspectos de suas operações. Como podem colher os benefícios dessa mudança digital sem se desviar do caminho devido a falhas em lidar com os desafios da segurança da informação?

A dinâmica do mercado fez com que a transformação digital se tornasse um problema em todas as áreas de uma empresa, envolvendo tecnologias que proporcionam maior valor aos seus clientes. Todas estas incorporações, que já começaram em muitas empresas há alguns anos, supõem, naturalmente, uma mudança cultural a nível organizacional que representam um grande desafio.

Obviamente, a segurança da informação não deve ser considerada como um item alheio a esta meta, mas como uma parte importante dos objetivos que as empresas devem estabelecer para não serem ignoradas nesta corrida pela segurança.

Como a transformação digital geralmente envolve uma reestruturação dos processos e estratégias de cada organização para aproveitar a tecnologia digital, isso abre novos perfis de risco que as empresas não podem perder de vista.

Mudanças em TI devem significar mudanças no gerenciamento da segurança

As empresas que já estão passando por processos de transformação digital têm se dedicado ao desenvolvimento de modelos de negócios que têm um alto componente tecnológico, o que obrigou as equipes de TI a ter que adaptar-se para suportar a velocidade dessas mudanças.

Todas estas modificações levam as empresas a passar gradualmente da centralização da maioria dos seus recursos para a contratação de uma ampla gama de serviços e ativos de apoio às atividades diárias, trazendo um aumento na

diversidade de tecnologias e plataformas sobre as quais o monitoramento deve ser feito.

Esse processo de transformação, que oito em cada dez organizações decidiram realizar nos últimos cinco anos, de acordo com uma pesquisa da [McKinsey](#), teve um impacto direto na segurança, o que obriga as empresas a reduzir suas chances de serem vítimas de um ataque cibernético ou de uma brecha de dados. Neste sentido, as equipes de gestão foram imersas em novos paradigmas que lhes permitem cumprir esta missão, mas sem afetar o funcionamento normal do negócio, uma vez que, para operar com sucesso neste ecossistema digital, as organizações devem ser capazes de proteger os dados durante este processo de transformação e nos respectivos ambientes.

De acordo com um estudo realizado pelo [Instituto Ponemon](#) em 2018 em diferentes países, 72% dos profissionais de segurança digital acreditam que a urgência de alcançar a transformação digital aumentou o risco de sofrer uma brecha de dados. Se acrescentarmos a isso o fato de que 45% das organizações disseram não ter uma estratégia para enfrentar a transformação digital, o cenário é pelo menos preocupante.

Para as equipes responsáveis pelo gerenciamento da segurança, um fluxo constante de informações em torno de todas as mudanças dentro da organização torna-se um requisito fundamental. É por esta razão que as tecnologias de inteligência e o monitoramento de ameaças são importantes para fornecer a base na qual outros processos podem ser executados de forma segura, mantendo o cumprimento de normas em toda a organização.

Variedade de tecnologias como mecanismo de mudança

Para as empresas é necessário considerar a segurança da informação como parte da digitalização de uma organização, e dado que existem múltiplas tecnologias que estão começando a ser consideradas para este processo, tais como computação em nuvem, plataformas móveis, conectividade 5G e machine learning, para citar apenas algumas; deve-se entender que não há apenas uma aplicação ou tecnologia que garanta a segurança dos dados e a continuidade dos negócios.

Certamente, para as empresas que já estão pensando no assunto, uma das principais dúvidas é por onde começar. E o ponto de partida é precisamente entender que toda essa transformação também está mudando radicalmente e muito rapidamente a sociedade global: a forma como trabalhamos, socializamos, compramos e interagimos com as múltiplas necessidades que fazem parte da vida cotidiana.

O caminho da mobilidade

Em todos estes cenários de mudança nas empresas, há um em particular que, até 2020, será um fator importante para acelerar todo este processo de transformação: a mobilidade laboral. Sem dúvida, a capacidade dos dispositivos de manter a conexão com as redes, independentemente de onde estejam, continua a expandir a superfície de ataque da qual um atacante pode se beneficiar.

Toda essa mudança já foi lentamente gerada nos últimos anos, mas a adoção cada vez mais acelerada pelas empresas do uso da tecnologia móvel é feita muitas vezes sem considerar a segurança. Portanto, é importante que as empresas não continuem considerando a segurança de uma forma clássica, mas sim que pensem em mudar para modelos adaptativos que possam responder às mudanças.

Além disso, as equipes de segurança devem aproveitar as tecnologias de monitoramento, uma vez que as tecnologias de detecção por si só não são suficientes. É importante que as empresas permitam que seus processos respondam a um incidente e retornem à operação, resolvendo incidentes e aplicando medidas corretivas adequadas.

Conceitos que devem ser mantidos na transformação digital

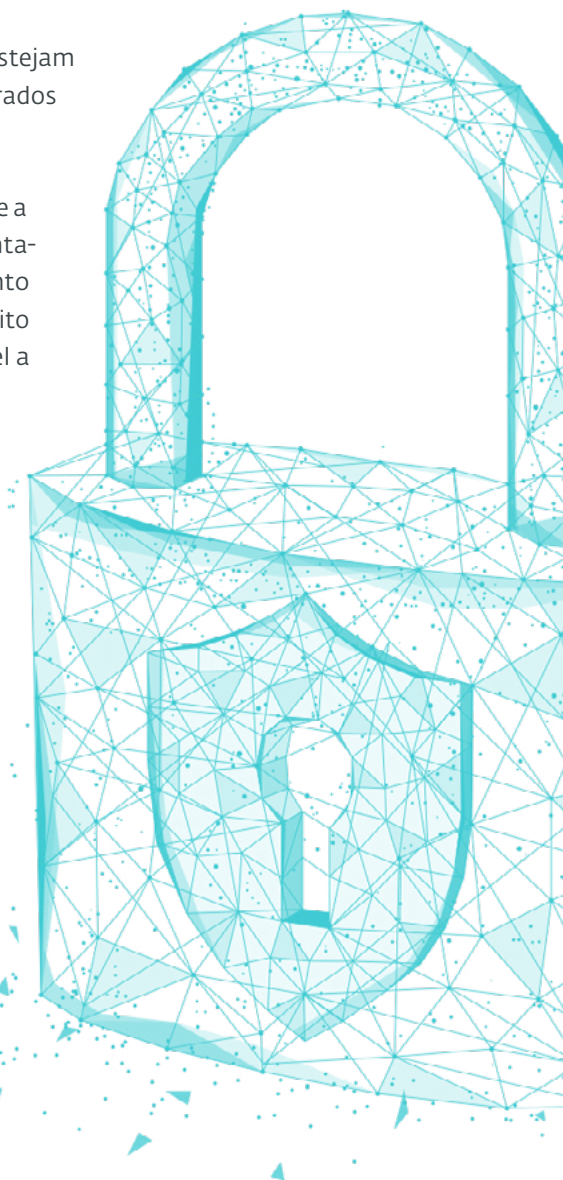
Para além de todas estas tecnologias específicas que continuarão evoluindo, não podemos perder de vista conceitos como a privacidade. Estamos em um momento em que estão surgindo cada vez mais leis novas e mais rigorosas em matéria de proteção de dados pessoais, o que faz com que as pessoas se tornem gradualmente mais conscientes dos seus direitos e mais interessadas na forma como as empresas podem administrar os seus dados.

Durante os próximos meses veremos como as organizações desenvolvem grandes mudanças em quase todos os níveis de seus negócios, tendo como eixo central a gestão da informação e dos dados próprios de sua operação. Neste cenário, os modelos de negócio que geram confiança por parte do cliente serão executados com vantagem.

Então, o que fazer nas empresas?

Diante do que as empresas enfrentarão no próximo ano, há pelo menos cinco considerações que devem ser levadas em conta para realizar essa transformação com segurança:

1. Procurar um equilíbrio entre a implementação de tecnologias e a cibersegurança. Se, desde o início, não houver equilíbrio e a segurança for também considerada como um fator dinamizador de negócios, os problemas serão maiores do que as soluções.
2. Desenvolver projetos que facilitem a visibilidade e o controle de tecnologias, de modo que o foco não seja apenas na prevenção de incidentes, mas que considerem a detecção e a resposta a um incidente.
3. O foco da segurança não pode ser apenas em dispositivos, já que temos cada vez mais equipamentos e tecnologias para implementar a segurança em cada componente de forma individual.
4. Incentivar uma maior colaboração entre pessoas e processos para que estejam alinhados e que a tomada de decisão seja baseada em dados comuns gerados a partir de tecnologias implementadas.
5. É claro que o componente humano não pode ser negligenciado. Dado que a transformação digital é algo que quase todas as pessoas têm experimentado em suas vidas diárias, embora muitas vezes com um comportamento arriscado em relação às suas informações pessoais, o trabalho deve ser feito para evitar que também a informação da empresa possa ser vulnerável a ataques de Engenharia Social.



CONCLUSÃO

Os desafios que temos pela frente são importantes e temos de nos preparar para que as gerações atuais e futuras tenham melhores ferramentas, tanto do ponto de vista tecnológico como educativo, para enfrentar os desafios apresentados pela segurança, pois só assim será dada à tecnologia a oportunidade de desenvolver o seu verdadeiro potencial e que isso se traduza em uma melhor qualidade de vida para a humanidade.


Como vimos em cada um dos capítulos que compõem este documento, o mundo pretende continuar evoluindo no uso da tecnologia e avançar para um mundo ainda mais “inteligente” do que o atual. Mas apenas quando os avanços da inteligência artificial realmente permitam que as máquinas pensem por si mesmas, quando a transformação para o que é conhecido como cidades inteligentes se torne um fenômeno global, e quando os processos de transformação digital pelos quais passam muitas empresas seja uma questão do passado, é que poderemos analisar com mais precisão quais foram os custos desse processo de transformação. O que é claro é que, à medida que a situação atual se apresenta, a segurança continuará estando um passo atrás na consideração dos desenvolvimentos tecnológicos e isso, possivelmente, trará consequências a curto prazo.

Embora existam sinais positivos que sugerem que alguns percebem a importância da segurança e a necessidade de que ela tenha um papel mais proeminente no futuro, se pensarmos que oito em cada dez empresas nos últimos cinco anos decidiram empreender o caminho da transformação digital e analisarmos o [crescimento das brechas de dados](#) a nível

global, para não mencionar o aumento dos custos que as empresas terão para lidar com este tipo de incidente de acordo com as [projeções](#), os números explicam as dificuldades que existem atualmente para evitar este tipo de incidente de segurança. Se também pararmos para pensar no crescimento projetado para a construção de edifícios e cidades inteligentes e que várias das cidades que atualmente apostam no conceito “Smart” têm sido vítimas de ameaças já conhecidas como o ransomware, porque devemos ser otimistas e pensar que o futuro será melhor em termos de segurança?

Nesta mesma linha, se tomarmos como referência os atuais avanços no uso do machine learning, o fenômeno das fake news e o que podemos esperar de um futuro ainda distante do desenvolvimento da inteligência artificial, o desafio de estarmos preparados para o que está por vir pode ser uma oportunidade para tomar medidas que realmente dêem à segurança um papel mais proeminente.

Desde 2016 até agora, as deepfakes nos deram sinais do possível impacto que podem ter com sua



participação em diferentes processos eleitorais, gerando grande confusão e incerteza sobre qual informação é verdadeira e qual é falsa; alimentando a desconfiança de indivíduos que, embora mais interconectados, continuam expondo dados e informações pessoais devido ao desconhecimento das boas práticas de segurança. Ao mesmo tempo, vários destes indivíduos terão de participar em processos eleitorais em países que preferem sistemas de votação eletrônico, apesar de terem demonstrado problemas.

Voltando à questão acima colocada, vimos sinais positivos que nos permitem ser otimistas. Empresas como o Facebook, universidades e outras importantes companhias têm demonstrado preocupação em combater fenômenos como as deepfakes com iniciativas como o lançamento do "[Deepfake Detection Challenge \(DFDC\)](#)", que visa promover o desenvolvimento de tecnologias capazes de combater o seu impacto. Além disso, como Lysa Myers explicou no capítulo "Mudanças substanciais em termos de privacidade", houve mudanças em questões legislativas e regulatórias que, embora tenham sido lentas e ainda não tenham gerado impacto relevante, são mudanças positivas no final.

Há ainda muito para ser feito e é fundamental a intervenção dos governos através de medidas que proporcionem uma orientação ou caminho a seguir. Apesar da falta de consciência que ainda existe por parte dos usuários em vários aspectos da segurança, a desconfiança e descrença que muitos manifestam são sintomas que refletem o conhecimento sobre o impacto da segurança e da privacidade em suas vidas, e isso também pode ser interpretado como uma oportunidade de continuar trabalhando em um fator-chave como a educação.

Grandes desafios estão por vir e temos que estar preparados, tanto a nível tecnológico como educativo, para que as gerações atuais e futuras disponham de instrumentos suficientes para poder enfrentá-los e para que a tecnologia tenha a oportunidade de expressar o seu potencial, proporcionando uma melhor qualidade de vida para os indivíduos.



CYBERSECURITY
EXPERTS ON YOUR SIDE