



CyberSec Predictions

Quem sou eu?

- _ Tecnólogo formado em Redes de Computadores pelo IBTA
- _ Pós graduado em Segurança da Informação pela FIA
- _ Trabalho com TI desde 1999 e com Cyber desde 2005
- _ Gerente Senior da KPMG, atuando com projetos de Cyber e Privacy



Cenário atual de Riscos cibernéticos



1) A tecnologia em casa é usada como uma porta de entrada para a empresa:

- Aumento exponencial do uso e da dependência de redes e dispositivos domésticos, algo que os cibercriminosos rapidamente perceberam.
- Para os invasores, essa mudança representou uma oportunidade única de explorar esses dispositivos e encontrar brechas nas empresas.
- Aumento exponencial de ataques de Phishing, principal fonte de entrada para Ransomware e demais vírus.

II. Ataques de ransomware ficam mais sofisticados

- O ransomware está oculto em mensagens, anexos e documentos relacionados à covid-19
- Se tornaram mais frequentes e continuam a se sofisticar.
- Proteção envolve uma abordagem integrada de cibersegurança: pessoas processos e tecnologia

Desafios atuais

O trabalho remoto levou a comprometimento das redes domésticas, e consequentemente as redes corporativas

- **OMS** lança avisos sobre **ataques de phishing via WhatsApp ou e-mail** com invasores representando a OMS
- Os **golpes de phishing com o tema COVID19** levaram a um aumento de **32% nos cyber crimes**

350%
+ ataques no
primeiro trimestre

Os golpes de Phishing do COVID aumentaram, comprometendo os e-mails pessoais e corporativos

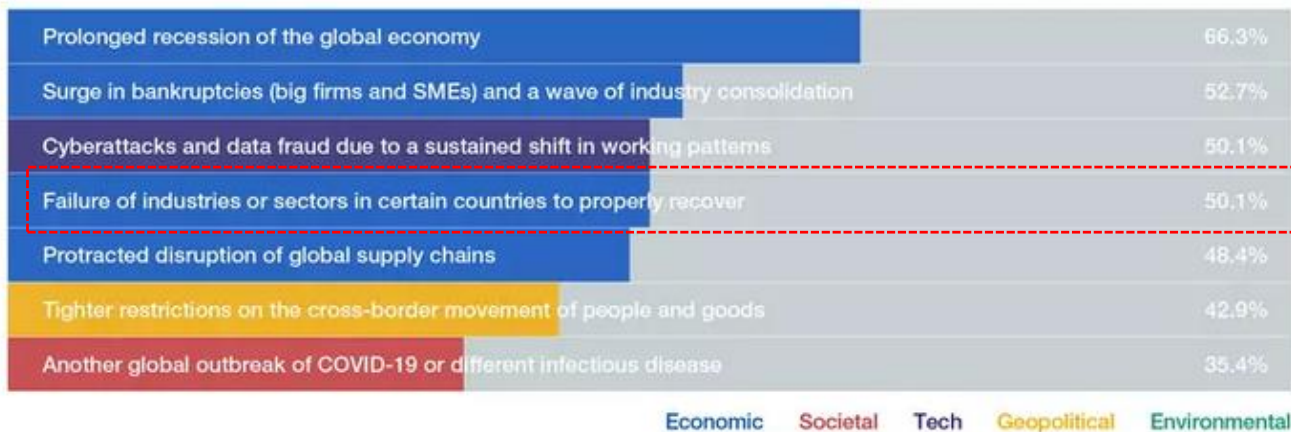
Infraestrutura crítica como hospitais e unidade fabris comprometidas

- Governo alemão, EUA e indiano, publicam consultoria sobre o uso do Zoom, destacando os riscos de privacidade e segurança
- Credenciais de usuários do Zoom vendidas na darkweb
- Cert-in reportou um surto de ataques cibernéticos em computadores pessoais desde o início do protocolo 'trabalho em casa'

Aplicações populares de vídeo conferência levam a falhas de Segurança Cibernética

Principais preocupações dos executivos WEF

Most worrisome for your company




What do business leaders think are the most worrisome risks to companies due to coronavirus?

Image: World Economic Forum

Visão de risco Sistêmico

Eventos com baixa Probabilidade e alto impacto são difíceis de se calibrar



Automação

The diagram features three overlapping circular elements, each composed of concentric rings in shades of blue, purple, and green. These circles are arranged in a triangular pattern. The background is dark blue with a faint, glowing network of white lines and dots, suggesting a global or digital connectivity theme.

Falta de visão de riscos cibernéticos em todas as linhas de defesa

Hyper
conectividade

Portfolio de riscos
associados a disrupção
tecnológica

Dispositivos conectados
anywhere

Interdependência
e criticidade

Aumento da intervenção
Regulatória: LGPD

Principais Riscos Cibernéticos



Office 365



E-commerce



Fraudes financeiras



Evolução do Ransomware



Supply Chain

“

Todos os dias, são perpetrados 8 trilhões de ataques, ao redor do globo. Sim, inacreditáveis 90 mil ações criminosas por segundo

Brasil teve 850 mil tentativas de ciberataques no terceiro trimestre de 2020

Se contarmos desde janeiro, esse numero sobe para 3,4 bilhões

Office 365



Ataques a senhas

- Automatização do “lembrar a senha”
- Reuso de senhas comprometidas anteriormente

Vazamento de dados

- Comprometimento das caixas de email
- Roubos e venda de dados pessoais
- Propriedade intelectual afetada

Alvo dos ataques

- Alta administração
- Rota de ataques para outras organizações

“

Exemplos de phishing

From: [Redacted]
Subject: Your Mailbox Will [Shutdown](#) Verify Your Account



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please [verify](#).

[Verify Now](#)

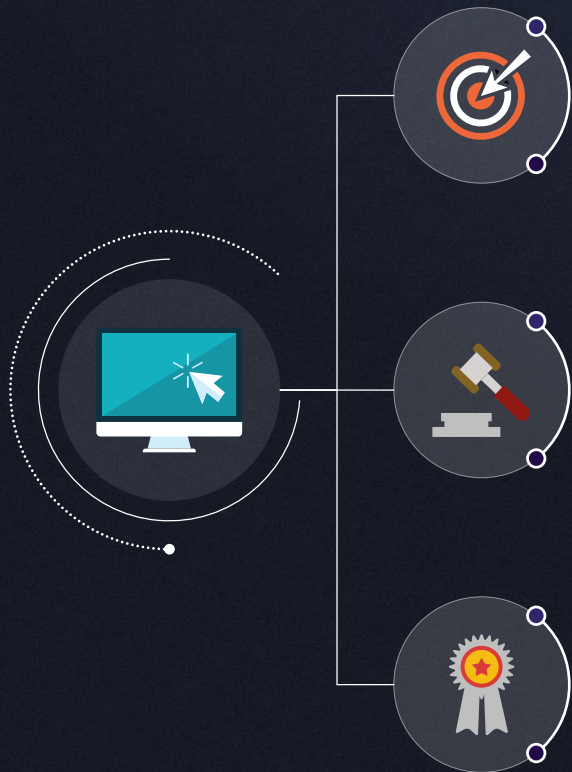
Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved



[Sign in](#)

[Can't access your account?](#)

Fraudes Financeiras



Spear Pishing

- Automatização da coleta de informações em redes sociais
- Construção de ataques sofisticados
- Uso de sites comprometidos

Escala Industrial

- Industrialização de ataques a CEOs
- Ataques a grandes call centers

Aumento da assertividade dos ataques

- Melhor compreensão dos modelos na industria
- E dos sistemas de controles de fraudes...

“

Até o dia 15/10/2020, De acordo com o Valor Investe, a CVM já havia recebido mais de 200 denúncias de fraudes financeiras

1. Falso site de cadastro do Pix
2. Assessor de investimento falso
3. Fraudes no cartão

Ransomware



Como serviço

- Ransomware sendo oferecido como serviço na darkweb
- Torna a execução do ataque mais simples e disponível

No devido tempo

- Invasores ficam mais tempo nos sistemas
- Cada vez mais roubando dados
- Foco: sistemas core e backup

Causando impactos

- Crescimento de ataques
- Vinculado a ameaças de divulgação de dados
- Interrupção nos negócios

“

O Brasil é o país mais atingido por ataques de ransomware em toda a América Latina.

+ de 2500 ataque desse tipo todos os dias

prejuízos variam na casa dos US\$ 700 mil dólares, envolvendo desde o pagamento de um possível resgate até danos à imagem ou relações com os clientes

A Evolução do Ransomware - BR

- 65% das organizações foram atacadas por ransomware;
- 36% das vítimas pararam o ataque antes do dados serem criptografados;
- 8% cujos dados foram criptografados recuperaram pagando o resgate;
- Custo somado para a recuperação dos dados foi de R\$ 2,55 milhões;
- 85% tem seguro de cibersegurança;
- 68% tem seguro de cibersegurança que cobre ransomware

Ecommerce



Scans Automatizados

- Automação de ataques
- Vulnerabilidades exploradas rapidamente
- Incluindo códigos de terceiros

Coleta de informações de pagamentos

- Skimmers inseridos nos websites
- Coleta em massa de dados de pagamentos
- Cartões de créditos vendidos na darweb

Escala do impacto

- Comprometimento dos cartões e aumento de fraudes
- Aumento de multas e penalidades - GDPR e LGPD
- Dano Reputacional as empresas

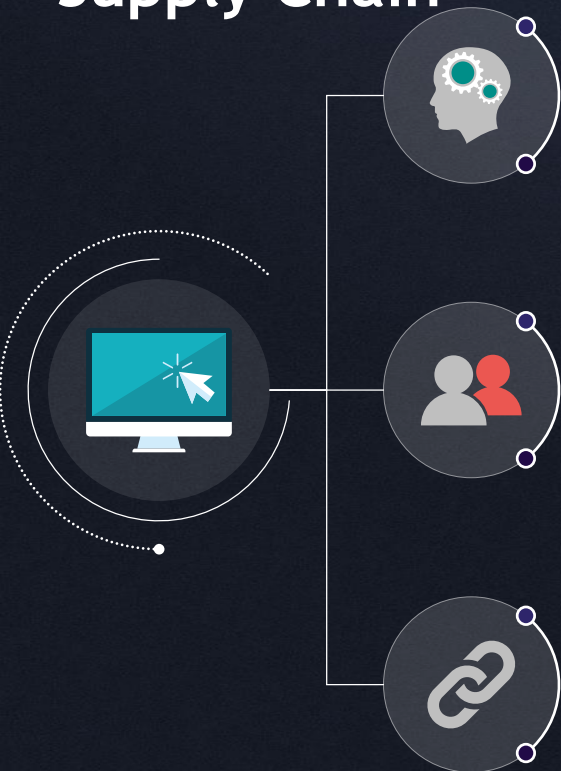
“

Inspiração para LGPD no Brasil, GDPR aplicou 395 multas na União Europeia

~ € 250MM em multas aplicadas

<https://www.enforcementtracker.com/>

Supply Chain



Provedores de serviços gerenciados

- Provedores de serviços gerenciados como alvo de ataques
- Comprometimento de diversos clientes

Provedores de softwares

- Provedores de SaaS alvo de ataques
- Dependência crescente de fornecedores

Sistemas Industriais

- Ambientes industriais (OT) em evidencia
- Riscos geopolíticos - Infraestrutura crítica

“

Ataque à TIVIT

Vazamento de dados em dezembro de 2018 que afetou credenciais de acesso de clientes — entre eles, Brasken, Banco Original, Zurich, Votorantim, Sebrae, SAP, Brookfield Energia, entre outros

+ de 30GB de dados

Como evitar?



85% dos ataques poderiam ser evitados, somente com a aplicação de 5 controles básicos:

- 1. Inventário e controle de Hardware**
- 2. Inventário e controle de Softwares**
- 3. Gestão de vulnerabilidades e patches**
- 4. Controle de privilégios administrativos**
- 5. Hardening de ativos**

<https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cis-controls/>



Porque tudo
isso acontece?





É SÓ O COMEÇO

[linkedin.com/in/fabioszescsik](https://www.linkedin.com/in/fabioszescsik)

Obrigado!

