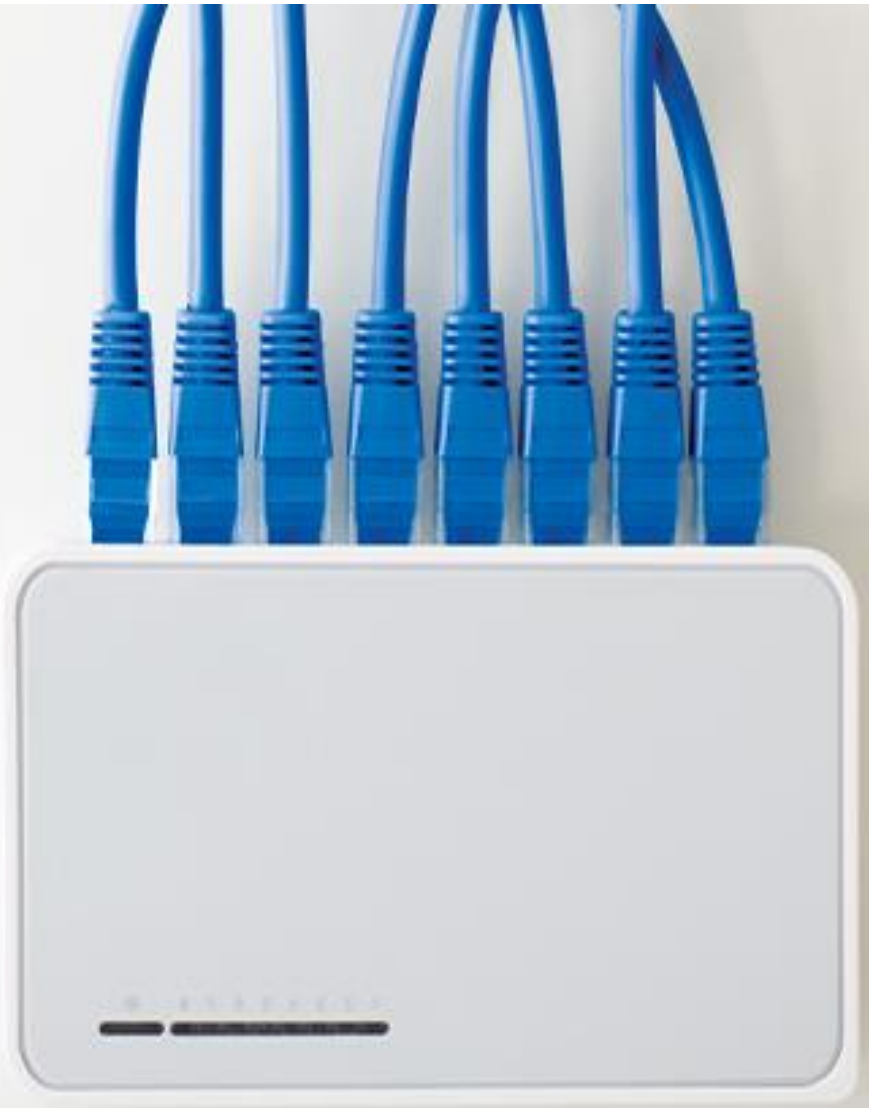
Desmistificando Ameaças Digitais



De

4º Risk Engineering Workshop
19 de Setembro de 2017

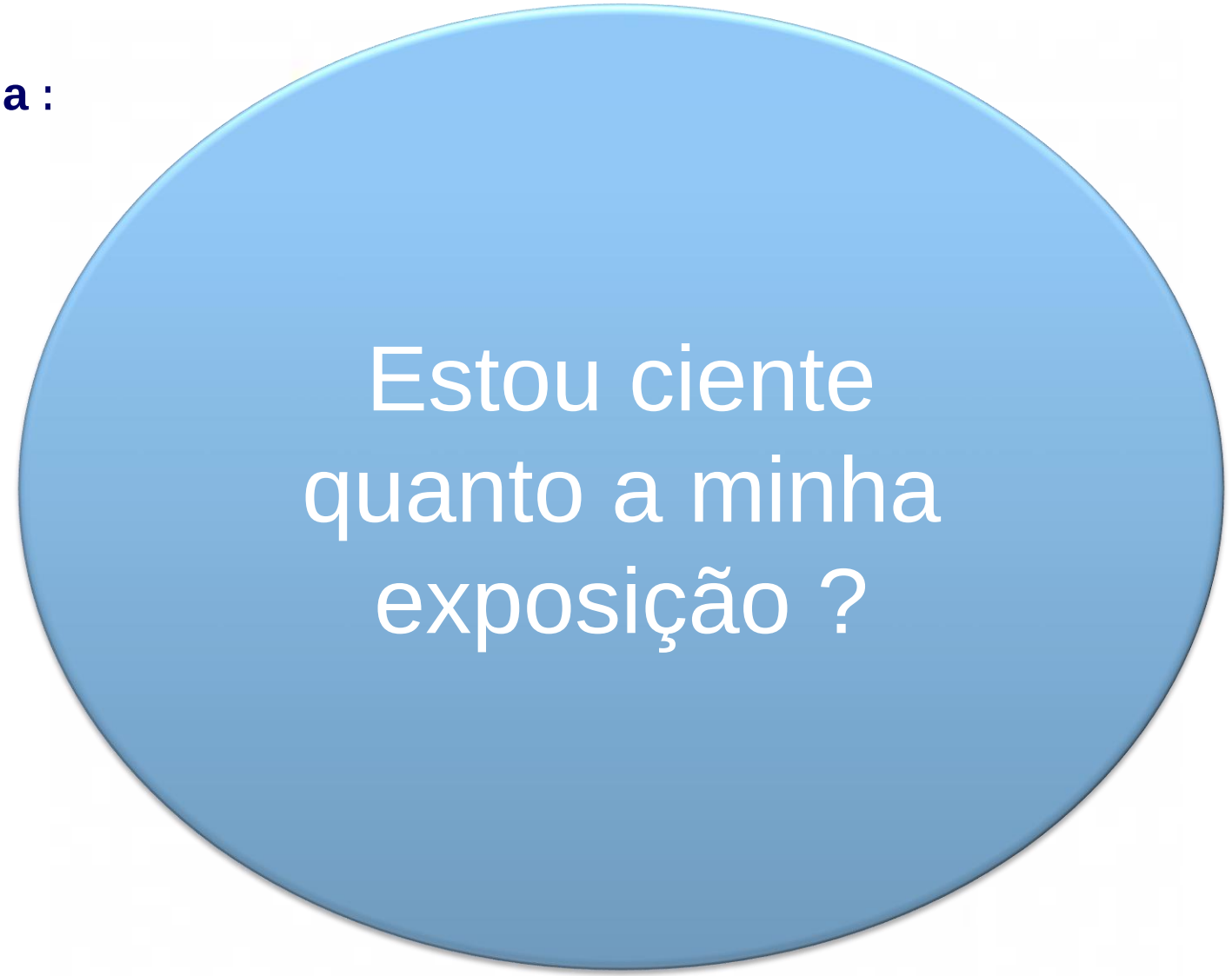
Tiago Santana – Eng. Cyber Risk
Risk Engineering

www.zurich.com.br

Brazil

Desmistificando Ameaças Digitais

Agenda :



Quiz Interativo

Empresas em que você trabalha ou trabalhou já sofreram algum tipo de ataque cibernético?

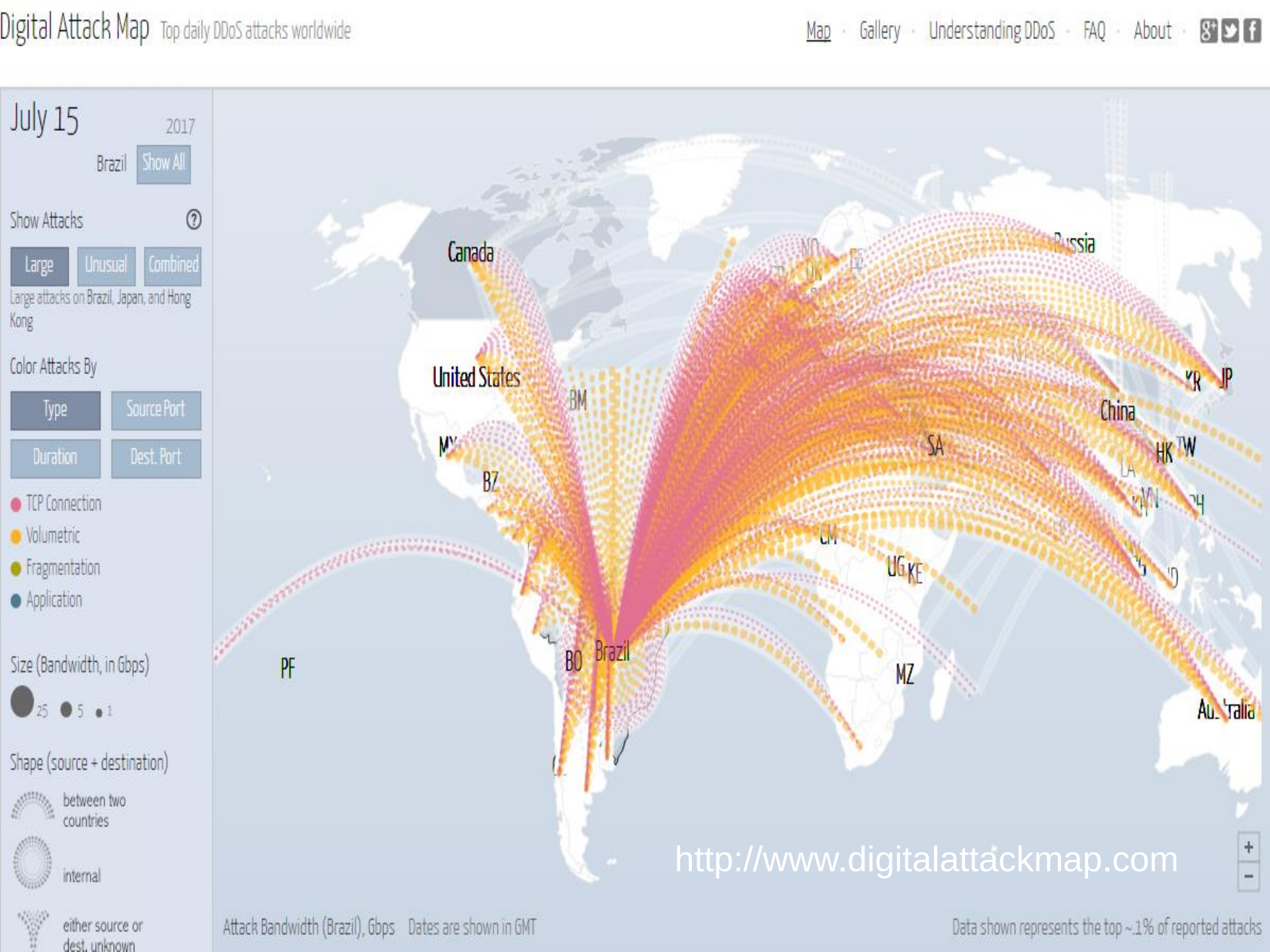
A) Nunca , tenho certeza absoluta.
B) Não sei, não tenho certeza.
C) Sim, ao menos uma vez.
D) Sim, duas ou mais vezes.

Quiz Interativo

Você acredita que os dados de sua empresa estão protegidos enquanto estamos nesse workshop?

A) Totalmente protegidos
B) Muito protegidos
C) Parcialmente protegidos
D) Pouco protegidos
E) Desprotegidos


CIBERAMEAÇA MAPA EM TEMPO REAL
PT
MAPA
ESTATÍSTICAS
FONTE DE DADOS
BUZZ
WIDGET
BRASIL
https://cybermap.kaspersky.com/pt/
10117085
13434108
363110
4176758
2530797
259582
13756587
0
OAS
ODS
MAV
WAV
IDS
VUL
KAS
BAD


Digital Attack Map
Top daily DDoS attacks worldwide
Map · Gallery · Understanding DDoS · FAQ · About
July 15
2017
Brazil
Show All
Show Attacks
Large
Unusual
Combined
Large attacks on Brazil, Japan, and Hong Kong
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
25
5
1
Shape (source + destination)
between two countries
internal
either source or dest. unknown
Canada
United States
Russia
China
Brazil
Australia
PF
BO
BZ
BM
SA
CM
UG
KE
MZ
JP
HK
TW
http://www.digitalattackmap.com
Attack Bandwidth (Brazil), Gbps
Dates are shown in GMT
Data shown represents the top ~1% of reported attacks

Principais Exposições

Eventos no Brasil

Duvulgações Hackers

Eventos no Brasil

ZURICH

zone-h unrestricted information

Home Notícias Eventos Fórum Arquivo Arquivo Onhold Notificar Estatísticas Registrar Login search...

Cópia salva em: 2017-08-20 04:28:02

Invadido por: dkr
Sistema: Linux
Domínio: https://egov.santos.sp.gov.br/siges/dkr.jsp
Web server: Apache
Endereço IP: 177.126.244.10
Estatísticas do Defacer

This is a CACHE (mirror) page of the site when it was saved by our robot on 2017-08-20 04:28:02

caiu na hackeado do

DKR

Você está sendo atacado nesse momento ?

ZURICH

Kroll Cyber Security

Fernando Carbone

Cyber Investigations Senior Director

Agora que você já sabe, vamos entender nosso risco!

Principais Exposições
Estatísticas

5% é o mínimo que uma empresa deveria aplicar do que investem em (TI) na segurança digital.

Stefanini Rafael

51% **das empresas brasileiras disseram ter sido vítimas de um ataque no ano passado**

.

Trend Micro

6º **Brasil é considerado o 6º país mais vulnerável a vírus que sequestra informações.**

Kaspersky

64,2 Mil **tentativas de invasões diárias ocorridas no Brasil no ano passado.**

Symantec

80% **dos ataques cibernéticos poderiam ser previnidos com ações simples como senhas seguras, configurações seguras, revalidações de acesso e gerenciamento de patching.**

National Audit Office - The UK cyber security strategy: Landscape review

80 **foram novos tipos de vírus que surgiram no ano passado**

Symantec

10

O Risco Cibernético é atualmente uma das 10 principais preocupações dos executivos no mundo

Relatório Global de Gerenciamento de Riscos, AON

96%

das vunerabilidades que afetam o Sistema operacional do windows poderiam ser mitigadas com simples restrições de perfis de administração

Avecto 2013 Microsoft Vulnerabilities Study

100%

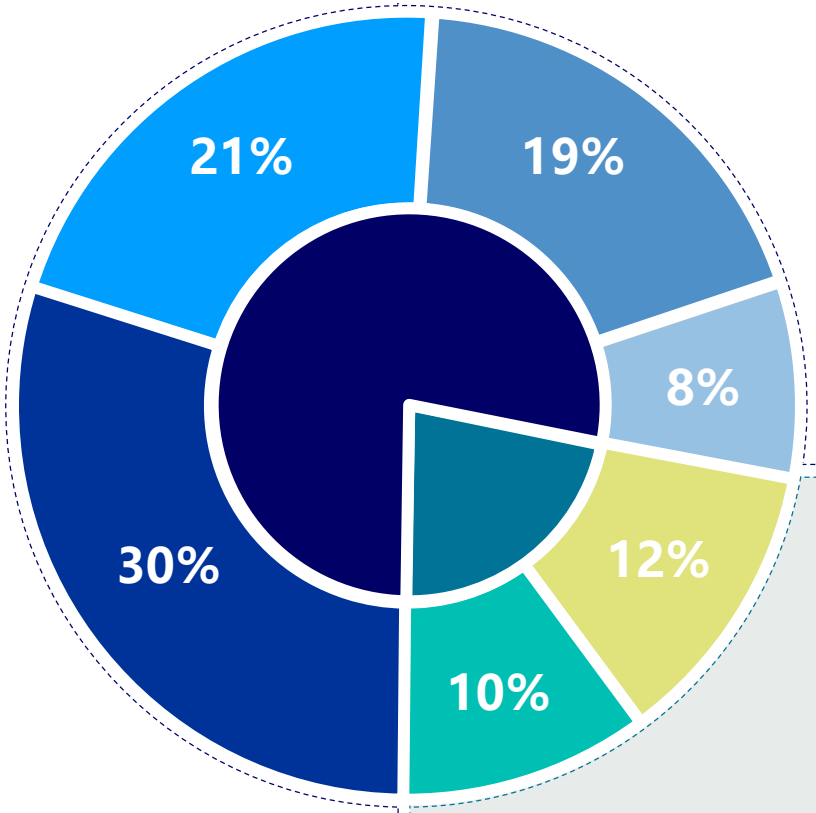
das invasões involvem furto de credenciais.

Mandiant

Principais Exposições
Cenário de ameaças Cibernéticas

ZURICH

Custos para as empresas



- Perdas em produtividade
- Lucros cessantes
- Custos de Compliance
- Risco reputaciaonal e danos à marca
- Custos com investigação Forense
- Custos co suporte técnico

Impactos de custos de TI

Data source: IBM Global Study on the Economic Impact of IT Risk

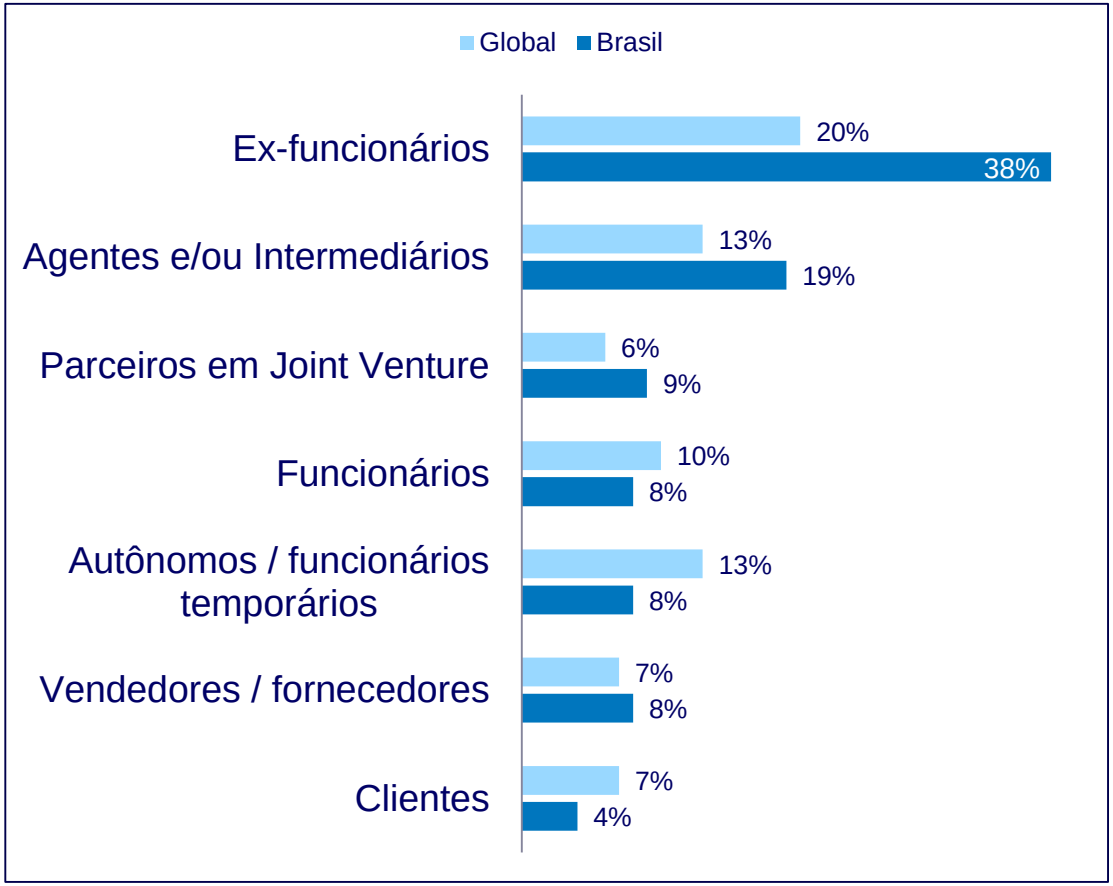
Como acontecem as os ataques cibernéticos?

Desmistificando Ameaças Digitais

Principais Perpetradores/Canais de Acessos

- Os principais responsáveis incidentes cibernéticos são funcionários e ex-funcionários das empresas

- Outros agentes são:
  - Crime organizado
  - Hacktivistas
  - Terrorismo
  - Script Kiddie



Fonte : Kroll

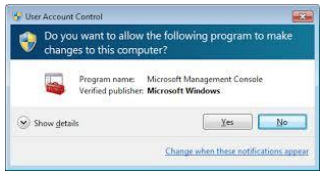
Desmistificando Ameaças Digitais

Como típico ataque cibernético funciona?

1 E-mail falso (phishing)

E-mail falso solciitando uma ação imediata.

2 Malware é executado



Usuário cliqua em um link e/or abre um anexo

3 Vazamento de dados, Extorsão

Malware permite acesso aos sites falsos, ou bloqueia arquivos no computador.

4 Limpeza de Rastros

Limpeza realizada pelo autor do malware, removendo todo os traços deixados.

Linha de Defesa

Processo	Pessoas	Tecnologia
• Resposta a Incidentes • Gestão de Mudanças • Monitoramento • Gestão de Atualizações • etc...	Treinamentos De Concientização	• Firewalls • Antivirus • Logs • Scan de Vulnerabilidades • etc...

Ataques reais acontecendo em todo lugar!

Exemplos reais recentes:

- Endereço não é do Banco;
- Clicando em qualquer local o malware é baixado.
- Informações de acesso são roubadas.

- Exemplo de Ransomware : resgate é solicitado para liberar dados do computador;
- Imposições são feitas de forma a pressionar a vítima.

Desmistificando Ameaças Digitais

Ataques Globais

Wannacry & Petya

12 de maio de 2017
300 mil comp. infectados
150 países afetados

27 de junho de 2017
80 mil comp. infectados
65 países afetados

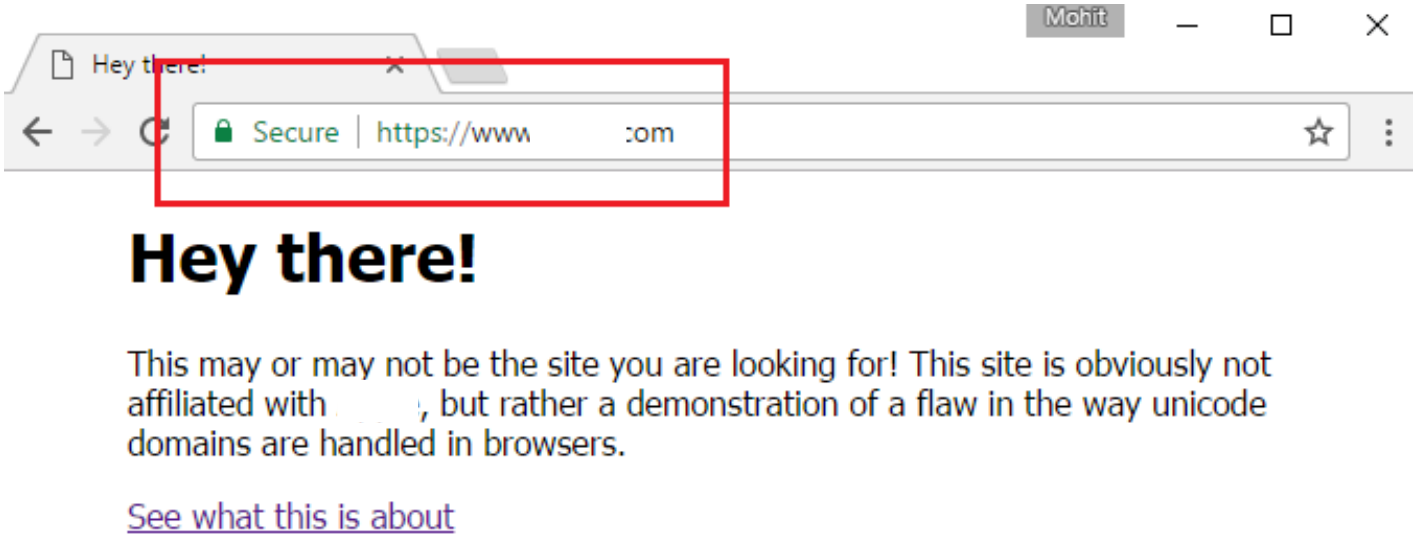
Organizações afetadas:

- Empresa de Telecomunicações (Brasil/Espanha)
- Hospital (Brasil)
- Saúde Publica (Colômbia/UK)
- Universidade (China/Itália)
- Montadora de Veículos (França/Romenia/UK)
- Ministérios (Romênia/Russia)
- Transportes (Rússia/Autralia/Holanda/UK)

- Geradoras de Energia (Ucrânia)
- Banco (Alemanha/Ucrânia/França)
- Ministérios (Romênia/Russia)
- Transportes (Rússia/UK)

Ataques sofisticados

Ataques Homograficos!



Como funciona o ataque:

- Usa caracteres Unicode para enganar as vítimas
- Endereço real em ASCII seria: https://www.xn--80ak6aa92e.com/
- Muito difícil de identificar!

Falta de Consciência de Segurança

Senhas Comuns

Top 15 - World 2016

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321
11. qwertyuiop
12. mynoob
13. 123321
14. 666666
15. 18atcskd2w

Fonte : Keeper Security

Top 15 - Brasil 2016

1. senha
2. 123456
3. 12345678
4. abc123
5. qwerty
6. amor
7. dragão
8. 111111
9. mestre
10. 123123
11. macaco
12. futebol
13. jesus
14. ninja
15. senha1

Fonte : Techmundo

Desmistificando Ameaças Digitais

ZURICH

Vamos refazer o quiz?

Quiz Interativo

Você acredita que os dados de sua empresa estão protegidos enquanto estamos nesse workshop?

A) Totalmente protegidos
B) Muito protegidos
C) Parcialmente protegidos
D) Pouco protegidos
E) Desprotegidos

Comparação

Como avaliar nossa exposição?

Avaliação de Riscos - Metodologia

National Institute of
Standards and Technology
Agência governamental

ETAPAS:

1. **IDENTIFIÇÃO** (O que proteger)
2. **PROTEÇÃO** (Como proteger)
3. **DETECÇÃO** (Logs & Alertas)
4. **RESPOSTA** (Plano & Prática)
5. **RECUPERAÇÃO** (Plano & Prática)

Avaliação de Riscos - CASE

1 – IDENTIFICAÇÃO:

- Dados são Classificados quanto a seus risco?
- Ativos da empresa são inventariados e validados?
- Governança & Segurança da Informação (Comites , BoD, KPIs)?

Avaliação de Riscos - CASE

2 – PROTEÇÃO:

- Ferramentas (AV/AM/Firewall/IDS/IPS/Web&Mail Filters/DLP)
- Dados sensíveis (pessoais/saúde/cartão de crédito)
- Controles de acessos (Senhas/2FA/MFA)
- Treinamentos de SI (Phishing, etc.)
- Procedimentos de Atualizações (Patching)

Avaliação de Riscos - CASE

3 - DETECÇÃO:

- Logs & SIEM (Security information and event management)
- Participação em comitês, grupos de discussões
- SOC (Security Operations Center) Interno ou Externo

Avaliação de Riscos - CASE

4 - RESPOSTA:

- Plano de Resposta a Incidentes (IRP) formalizado
- Testes e Atualizações periódicas do IRP
- Contratos com Terceiros para suporte de Incidentes

Avaliação de Riscos - CASE

5 - RECUPERAÇÃO:

- BCP e DRP formalizado
- Procedimentos de Backups
- Data Center alternativos (hot, cold)

Dicas simples e práticas

Desmistificando Ameaças Digitais

Mantenha-se seguro online!

- Não envie informações pessoais ou financeiras por e-mails e não responda a e-mails que solicitem essas informações;
- Antes de enviar informações sensíveis pela internet, verifique se o website é seguro;
- Preste atenção nos endereços dos sites. Sites maliciosos podem parecer idênticos aos legítimos, mas podem usar variações de escrita do domínio (ex: App1e.com);

PARE, PENSE, PROCEDA:

- Quando em dúvida, jogue fora: se o e-mail/mensagem parecer suspeita, é melhor apagar.
- Pense antes de agir: Fique atento a mensagens que solicitam ações imediatas ou ofereçam algo muito bom para ser verdade;
- Proteja sua senha: Senhas são como escova de dentes – não compartilhe com ninguém e substitua frequentemente;
- Conta única, senha única: Evite usar a mesma senha em vários sistemas/serviços, ao menos, não para a mesmo ambiente (corporativo, financeiro, pessoal , etc).

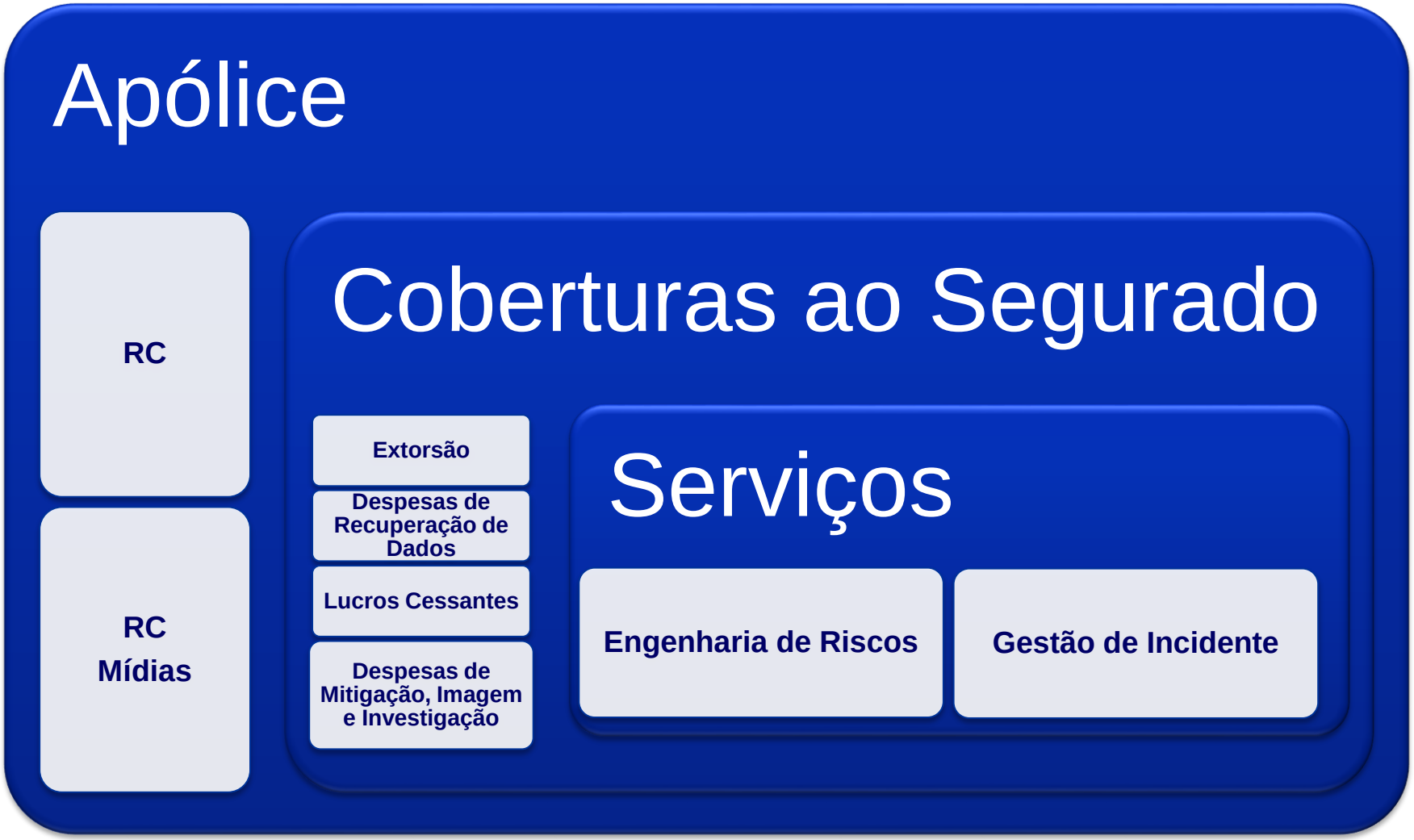
Zurich Proteção Digital

Segurança e Privacidade dos dados do seu negócio

Profissionais capacitados

Equipe especializada

Zurich Proteção Digital



Zurich Proteção Digital
Risk Assessment - Benefícios

CLIENTE

- Sem custos adicional
- Avaliação quanto à maturidade da segurança
- Sugestões para a melhorias
- Adequação das coberturas a realidade do cliente
- Suporte para dúvidas

CORRETOR

- Entendimento do risco do ponto de vista técnico
- Guiar o segurado na apresentação da proposta
- Suporte para dúvidas técnicas de segurança da informação e TI.

Engenharia de Riscos

Zurich Proteção Digital

Risk Assessment and Risk Improvement

Zurich Proteção Digital

Informações Adicionais

Endereço: www.zurich.com.br

Obrigado !