PROTEÇÃO DE DADOS NO BRASIL

Audiência Pública

Altair Olivo Santin
CESeg: Comissão Especial em Segurança da Informação e de Sistemas Computacionais

CÂMARA DOS DEPUTADOS
Comissão de Defesa do Consumidor

18.06.2019

Agenda

- Investimento em Segurança da Informação
- Cenários de Violação de Segurança
- Investimento em Privacidade da Informação
- Cenários de Violação de Privacidade
- Considerações
- Necessidades para mudar o futuro
- Referencial Curricular do bacharelado em CiberSegurança

Segurança em Redes e Sistemas Operacionais

Segurança em Comércio Eletrônico

Uso de Criptografia

Investimento em Capacitação / Treinamento de Pessoal

Boas Práticas, baseadas em Normas

Governança de TI com Processos para Segurança da Informação

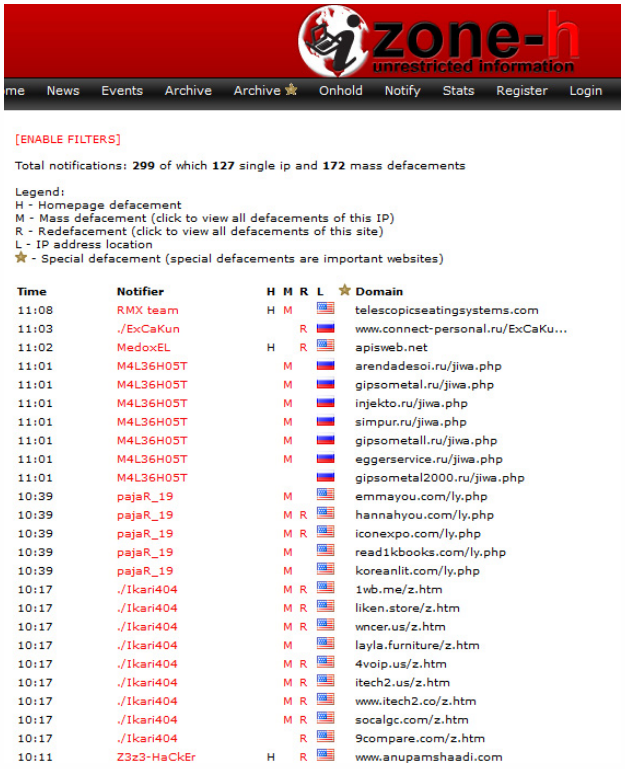
Investimento em Segurança da Informação

Lado Empresa

Overall email malware rate

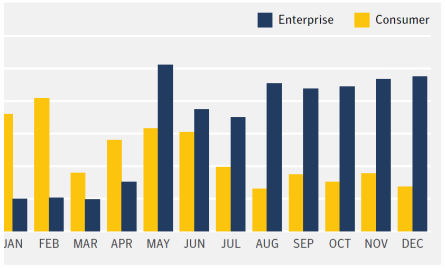
In 2017, the rate for email-borne malware fell to 1 in 412 (0.2 perce from 1 in 131 (0.8 percent) in 2016.

Year	1 in
2015	220
2016	131
2017	412



e vs. consumer ransomware detections by month

nsomware attacks against consumers dominated in the early part cs against enterprises dominated following the WannaCry May.



Overall phishing rate

The phishing rate declined from 1 in 2,596 in 2016 to 1 in 2,995 in 2017.

Year	1 in
2015	1,846
2016	2,596
2017	2,995

Cenários de Violação de Segurança

Fonte: Symantec Internet Security Threat Report 2018

Malware

92%
Increase in new downloader variants

80%
Increase in new malware on Macs

8,500%
Increase in coinminer detections

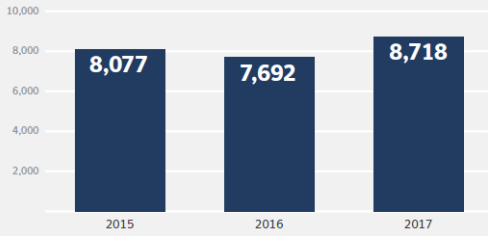
IoT attacks by source country

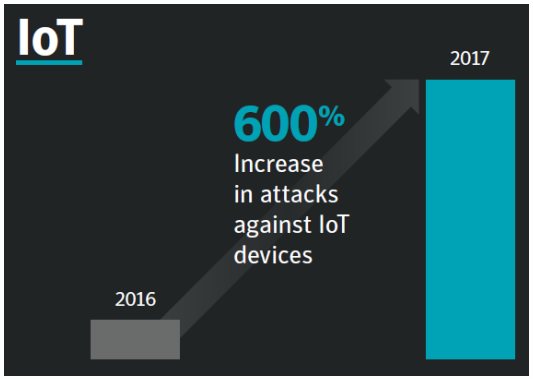
This table shows the country of origin, based on IP address, of the attacking devices.

Rank	Country	2017 Percent	Country	2016 Percent
1	China	21	China	22.2
2	United States	10.6	United States	18.7
3	Brazil	6.9	Vietnam	6
4	Russian Federation	6.4	Russian Federation	5.5
5	India	5.4	Germany	4.2
6	Japan	4.1	Netherlands	3
7	Turkey	4.1	United Kingdom	2.7
8	Argentina	3.7	France	2.6
9	South Korea	3.6	Ukraine	2.6
10	Mexico	3.5	Argentina	2.5

Total number of vulnerabilities

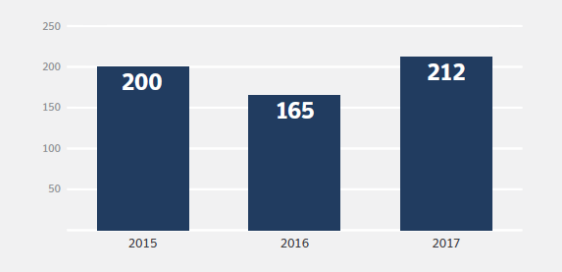
This shows a 13 percent increase in the number of reported vulnerabilities recorded in 2017.





Vulnerabilities disclosed in industrial control systems

There was an increase of 29 percent in the number of recorded vulnerabilities affecting industrial control system (ICS) technology in 2017.



Cenários de Violação de Segurança

Fonte: Symantec Internet Security Threat Report 2018

Data Privacy Officer | Time interdisciplinar

Desenvolvimento de Cultura de Privacidade

Inventário de dados | política de retenção de dados / backup

Revisão / Ajuste de Contratos | Código de Conduta para Proteção de Dados

Gestão de Consentimentos | Política e avisos de Privacidade

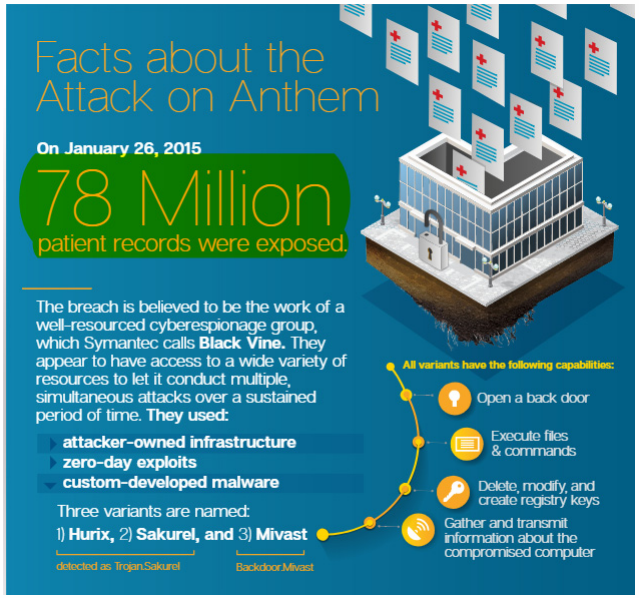
Ferramentas de *Compliance* / Privacidade (e.g. Nymity)

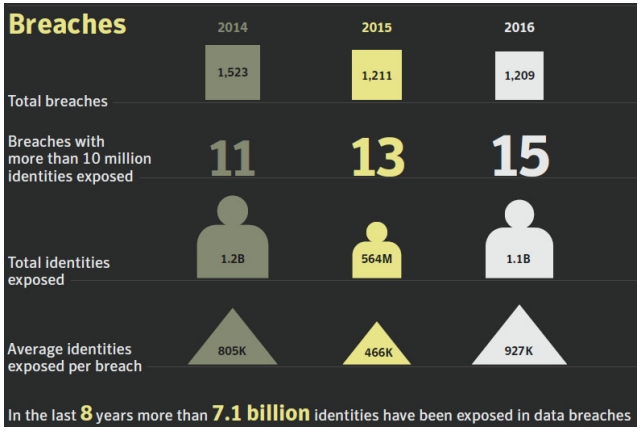
Resposta a incidentes / violações de Privacidade / Dados

Processo custoso e continuo, mas necessário

Investimento em Privacidade da Informação

Baseado na LGPD





Cenários de Violação de Privacidade

Fonte: Symantec Internet Security Threat Report 2016 e 2017

As empresas que oferecem novas tecnologias não se preocupam com segurança, num primeiro momento

Pessoas são “seduzidas” a usar novas tecnologias, mas em geral não avaliam os riscos de segurança

Pessoas cometem os mesmos erros ou erros similares no transcorrer do tempo

Mesmos ataques continuam funcionando, em diferentes tecnologias

Novos ataques /violações de segurança / Privacidade surgem constantemente

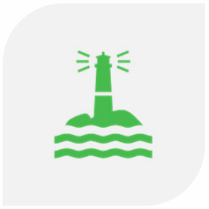
O número de relatos de ataques /ou violações bem sucedidos aumenta sempre

Considerações

Segurança e Privacidade da informação **são ortogonais em vários aspectos** e precisam de tratamento diferenciado

Segurança e Privacidade da informação **ainda não são concebidas e incorporadas ao projeto de sistemas desde o seu início (*by design)***

Sistemas falham porque os **ambientes** tecnológicos são e serão cada vez mais **heterogêneos e complexos**



Pessoas não são treinadas para lidar com as necessidades de segurança e privacidade e, em geral, também não sabem o que exigir dos sistemas que usam

A estimativa é que em 2022 haja algo como **1.8 milhões* de vagas de emprego não preenchidas** na área de CiberSegurança no mundo

*www.csoonline.com/article/2953258/it-careers/cybersecurity-jobmarketfigures-2015-to-2019-indicate-severe-workforce-shortage.html

Considerações

Necessidades para mudar o futuro

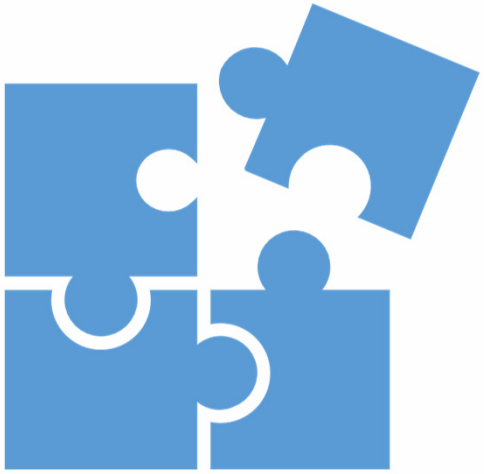
Investimento forte em formação de profissionais, pesquisadores e graduados, em cursos de segurança e privacidade da informação

Investimento forte e contínuo em capacitação de educadores para termos futuros jovens conscientes de necessidades de segurança e privacidade

Investimento forte e contínuo em **capacitação da população, desenvolvimento de campanhas de conscientização, em especial para pessoas "tecnologicamente vulneráveis"**

Incentivo forte e contínuo à **pesquisa, desenvolvimento e inovação, para melhorar a competitividade do país no mercado mundial**

Representação da CESeg e demais comissões especiais da SBC na ANPD



O Referencial Curricular (RF) esta em elaboração e considera os seguintes aspectos de Segurança:

Segurança de Dados

- conceitos básicos de criptografia, comunicação seguras fim-a-fim, forense digital, integridade de dados e autenticação e exclusão de dados

Segurança de Software

- princípios fundamentais de desenvolvimento e implementação, analise e testes, *deploy* e manutenção, documentação e ética

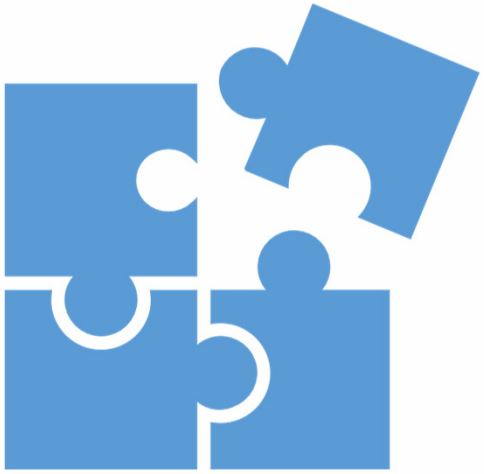
Segurança de Componentes

- vulnerabilidade dos sistemas de componentes, obtenção de componentes, teste de componentes, engenharia reversa de componentes

Segurança de Conexão

- mídia física, interface física e conectores, arquitetura de hardware, arquitetura de sistemas distribuídos, arquitetura de rede de computadores, segurança de sistemas, implementação de rede de computadores, serviços de redes de computadores e defesa de rede de computadores

CESeg | Referencial Curricular do bacharelado em CiberSegurança



Segurança de Sistemas

- *system thinking*, segurança de software, manutenção de sistemas, acesso a sistemas, controle de sistemas, arquitetura comum de sistemas, conexão segura

Segurança de Pessoas

- gestão de identidade, engenharia social, conformidade pessoal com normas de cibersecurity/regras/políticas/ética, conscientização e entendimento, privacidade social e comportamental, segurança e privacidade de dados pessoais, e privacidade e segurança usável

Segurança organizacional

- gestão de risco, política e governança de segurança, privacidade de dados, leis, ética, conformidade, ferramentas de analítica, administração de sistemas, planejamento de cibersegurança, continuidade do negócio, desastre e recuperação e gestão de incidentes, gestão de programa de segurança, segurança pessoal, segurança de operações

Segurança Societal

- abrange o espectro global de: cibercrimes, direito digital, ética digital, políticas digitais e privacidade

O RF é inspirado no documento da iniciativa internacional do GRCC, "Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity" (http://cybered.acm.org/).

CESeg | Referencial Curricular do bacharelado em CiberSegurança

http://www.sbc.org.br

altair.santin@pucpr.br

SBC
Sociedade Brasileira de Computação

sbc@sbc.org.br