Segurança Cibernética no Setor Elétrico

Agenda

- Segurança Cibernética na OSIsoft
- O desafio da Segurança Cibernética no contexto da necessidade de aumento da eficiência nas organizações
- A defesa em profundidade e sua relação com as principais normas internacionais – ISA/IEC 62443, IEC 62351 e NERC/CIP
- Uma contextualização sobre o futuro da Segurança Cibernética nas organizações
- Sessão de Perguntas

Luiz Kawafune

- Engenheiro Eletricista com atuação na área de Sistemas de Controle e Automação.
- Especialista em Segurança Cibernética da OSIsoft América Latina.
- 10 anos de experiência na área de geração e transmissão de energia, atuando nas áreas de Sistemas SCADA, Infraestrutura de Redes de Automação e Controle e Segurança Cibernética.
- Algumas publicações:
  - Segurança Cibernética em Redes de Automação e Controle – XI SIMPASE (2015)
  - Defesa em Profundidade para Redes de Automação e Controle: Mais do que firewalls – XII SIMPASE (2017)

Segurança Cibernética na OSIsoft

https://techsupport.osisoft.com

A necessidade da integração entre os domínios

Rede Operativa

Sala de Controle

Infraestrutura
de Rede

Galeria Elétrica

Rede Corporativa

DEC/FEC
(Duração/Frequência
de Interrupção)

ERAC
(Esquema Regional de
Alívio de Carga)

PCMC
(Plano de Corte
Manual de Carga)

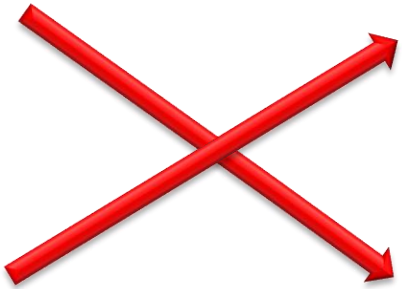
Plano de Geração

Cálculo de Capacidade

O Paradigma da Segurança

Redes Corporativas

- Confidencialidade
- Integridade
- Disponibilidade



Redes Operativas

- Disponibilidade
- Integridade
- Confidencialidade

Mitos da Segurança Cibernética

- Negação:
  - “Ninguém iria querer nos atacar”
  - “Isso não acontece conosco”
- Transferência de Responsabilidade:
  - “Isso é um problema do TI”
  - “Segurança Cibernética operacional é a mesma coisa da corporativa”
- Ingenuidade:
  - “Segurança Cibernética é um projeto”
  - “Conseguimos eliminar todas as nossas vulnerabilidades”
  - “Incidentes de segurança não afetam nossas operações”

Não existem redes isoladas

- Quão “isoladas” estão as suas redes?
  - Pontos de conexão com outras redes
  - Dispositivos removíveis
  - Aplicações que realizam acesso/extração de dados
- Pontos de conexão (de qualquer natureza) devem ser considerados como potenciais vetores de ataque
- Você não necessita estar conectado a internet para ter o risco de ser vítima de um ataque cibernético

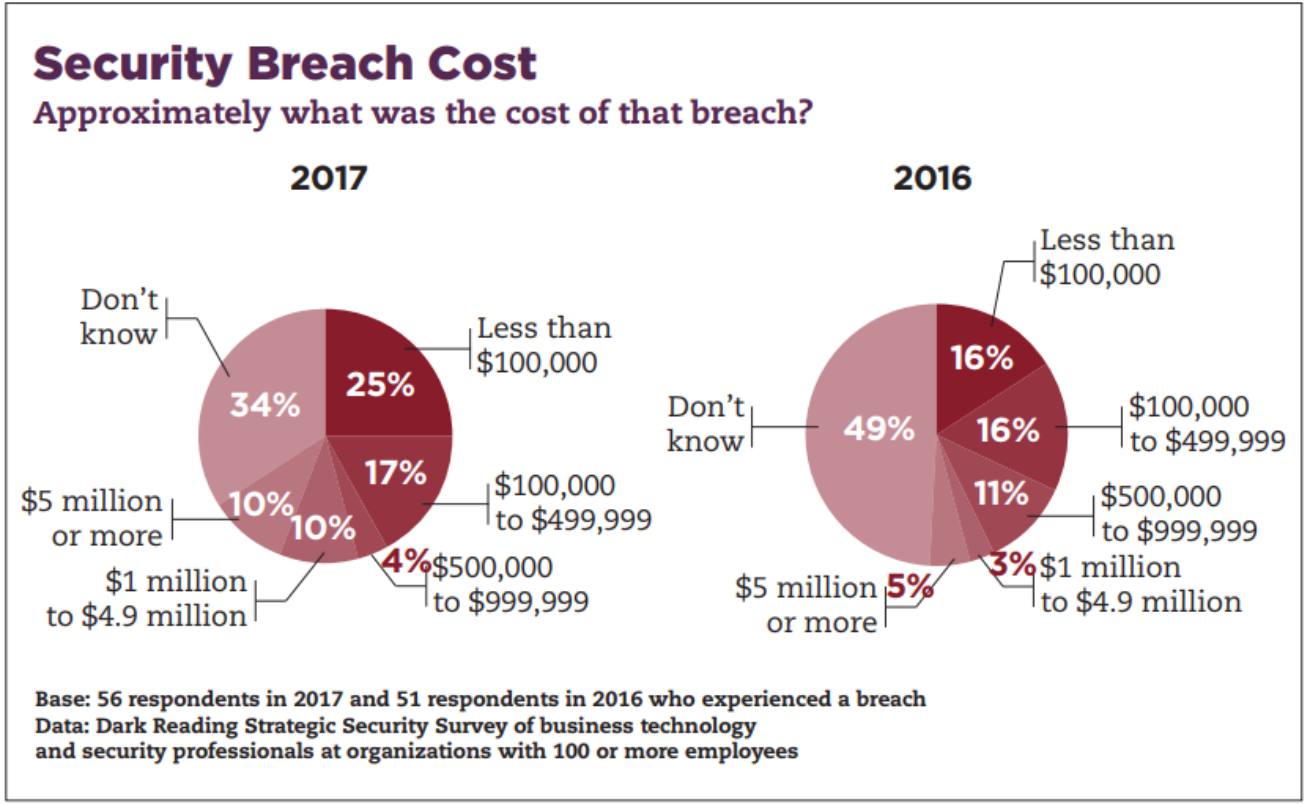
Segurança pela obscuridade

- É contar com a confidencialidade das informações de um sistema como indicador de segurança
  - “Se minha arquitetura não é conhecida, não posso ser atacado”
  - *“Os trapaceiros são muito bons em sua profissão e já sabem muito mais do que podemos lhes ensinar”* – Hobbs, A. C., 1851
- Diversas organizações internacionais (como, por exemplo, NIST e NERC) desencorajam e não recomendam a utilização desta técnica como metodologia de segurança

Quão grande é o problema?

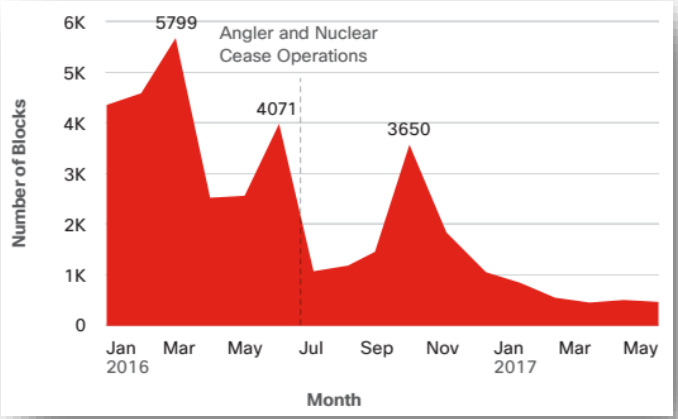
Perfil dos Ataques
- 65% Malware
- 55% Phishing

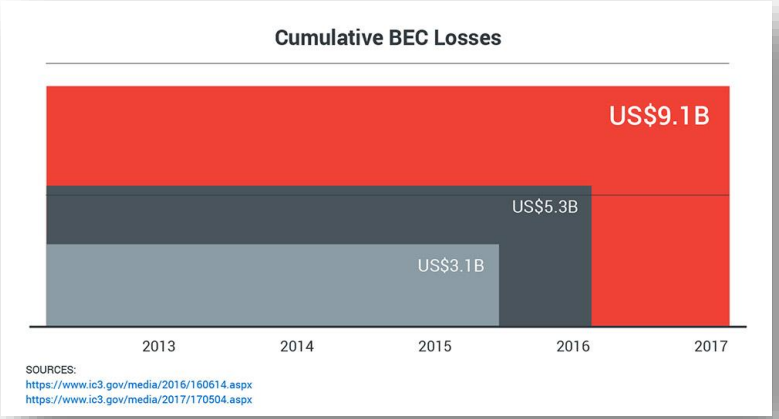
50% dos ataques usaram vulnerabilidades conhecidas e já corrigidas por meio de patches



Mudanças nos Perfis de Ataque em 2016/2017

- Os ataques utilizando exploit-kits tiveram redução de aproximadamente 77% entre 2016 e 2017
- As perdas por ataques utilizando e-mails corporativos como vetor tiveram aumento de aproximadamente 72% entre 2016 e 2017





Fontes: Cisco 2017 Midyear Security Report e FBI/IC3

Segurança Cibernética e IoT

- Ataques utilizando infraestrutura IoT capturada nos levam a era 1Tbps-DDoS
- O grande desafio de IoT atualmente é a **visibilidade**: Os defensores sequer sabem quantos dispositivos de IoT estão conectados às suas redes
- Vulnerabilidades presentes nestes dispositivos permitem que um atacante atravesse rapidamente diversas redes sem ser detectado
- Ao conseguir capturar dispositivos de IoT, um atacante consegue formar um botnet com mais de 100.000 dispositivos, tipicamente, em 24 horas
- O malware possui um índice de detecção baixíssimo uma vez que seu código reside em memória e é apagado assim que o dispositivo é reiniciado

O “Mirai”

- Este malware pode utilizar até 10 métodos de ataque com o mesmo código, alguns altamente sofisticados

```
#define ATK_VEC_UDP         0  /* Straight up UDP flood */
#define ATK_VEC_VSE         1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS         2  /* DNS water torture */
#define ATK_VEC_SYN         3  /* SYN flood with options */
#define ATK_VEC_ACK         4  /* ACK flood */
#define ATK_VEC_STOMP       5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP       6  /* GRE IP flood */
#define ATK_VEC_GREETH      7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY       8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN   9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP        10 /* HTTP layer 7 flood */
```

Source: Radware

Defesa em Profundidade

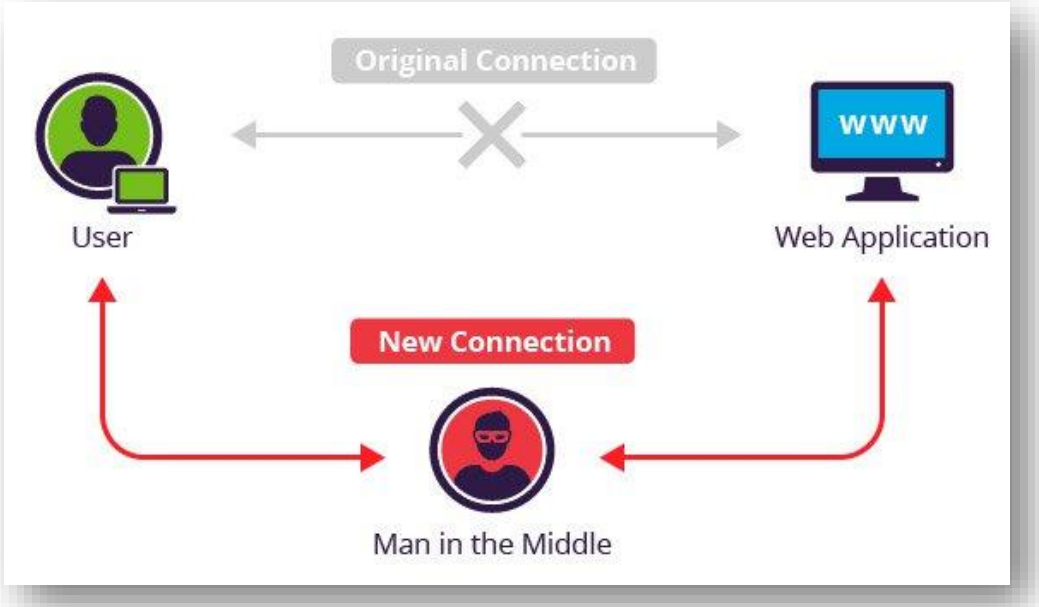
- Baseado no mesmo conceito utilizado em táticas militares: Cria barreiras para parar ou atrasar um adversário durante um ataque
- Este modelo visa ampliar o perímetro de defesa aplicando mecanismos de controle de escopo local, reduzindo a chamada “Superfície de Ataque”

Backup e Restauração

- Tem influência direta no tempo de recuperação em caso de ataque
- Deve estar documentado e associado ao Plano de Resposta a Incidentes
- Os procedimentos podem variar, de acordo com a norma escolhida como referência
- Algumas referências:
  - NIST Security Framework
  - NERC/CIP-009-6
  - IEC 62443-3-3
  - IEC 62351-10 aborda adicionalmente a questão da criptografia dos dados de backup

Criptografia do Tráfego de Rede

- O objetivo é mitigar ataques do tipo “Man-In-The-Middle”
- O tráfego é validado a partir de TLS para TCP/IP usando certificados X.509 para autenticação
- Algumas referências:
  - IEC 62351-3

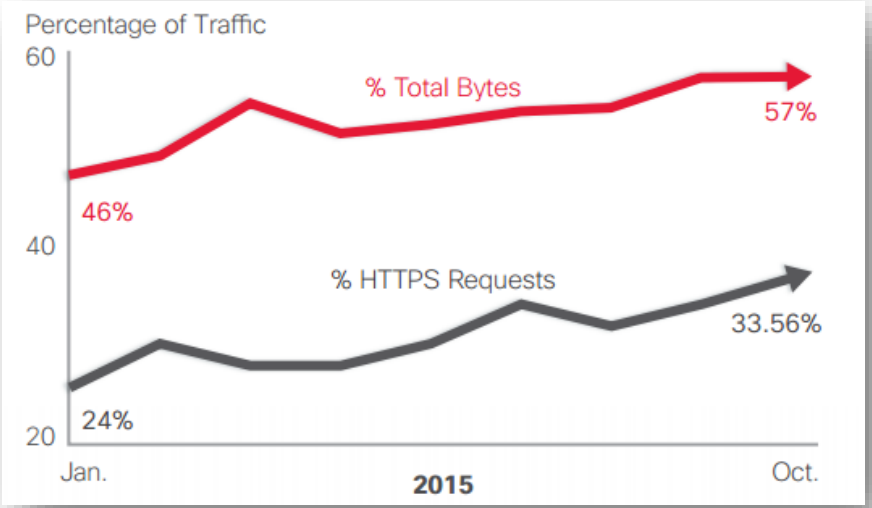


Segurança X Confidencialidade

- Observa-se que os atacantes estão utilizando cada vez mais criptografia para esconder ações em curso
- Aproveitam-se do fato das comunicações entre dispositivos não estarem criptografadas ou protegidas

Lembre-se sempre:

- Criptografia = **<u>Confidencialidade</u>**
- Criptografia quando combinada com outros elementos, provê segurança



Fonte: Cisco 2016 Annual Cyber Security Report

Application Hardening

- Configurar e habilitar apenas as funções/serviços que serão utilizados em uma aplicação
- Defina e configure as permissões necessárias às aplicações
- Mantenha todas as aplicações (inclusive sistemas operacionais) com suas versões mais atualizadas
- Algumas referências:
  - NERC/CIP-007-6
  - IEC 62443-2-4

Permissões Mínimas em Contas de Serviço

- Utilizar, sempre que possível, contas de serviço para aplicações com permissões mínimas – acesso somente aos recursos necessários
- Assim como os serviços, usuários devem seguir as mesmas regras de mínimas permissões
- A utilização desta estratégia reduz drasticamente o efeito de ataques utilizando crypto-ransomware
- Algumas referências:
  - NERC/CIP-007-6
  - IEC 62443-2-4
  - IEC 62443-3-1

Técnicas de Whitelisting X Blacklisting

- **Blacklisting:** Trata-se de ativamente bloquear o acesso a uma determinada aplicação/serviço/porta
- **Whitelisting:** Trata-se de ativamente permitir o acesso a uma determinada aplicação/serviço/porta
- Atualmente recomenda-se em termos de segurança cibernética a utilização de técnicas de whitelisting, tendo em vista que esta técnica é mais proativa

Whitelisting de Aplicações

- Utilizar ferramentas de whitelisting de aplicações para permitir a execução apenas de aplicações autorizadas
  - Windows: AppLocker
  - Linux: Integrity Measurement Architecture, Module Signing e Secure Boot
- A utilização desta estratégia reduz drasticamente o efeito de ataques utilizando crypto-ransomware
- Algumas referências:
  - NIST Application Whitelisting Guide 800-167
  - NERC/CIP-007-6
  - IEC 62443-3-3

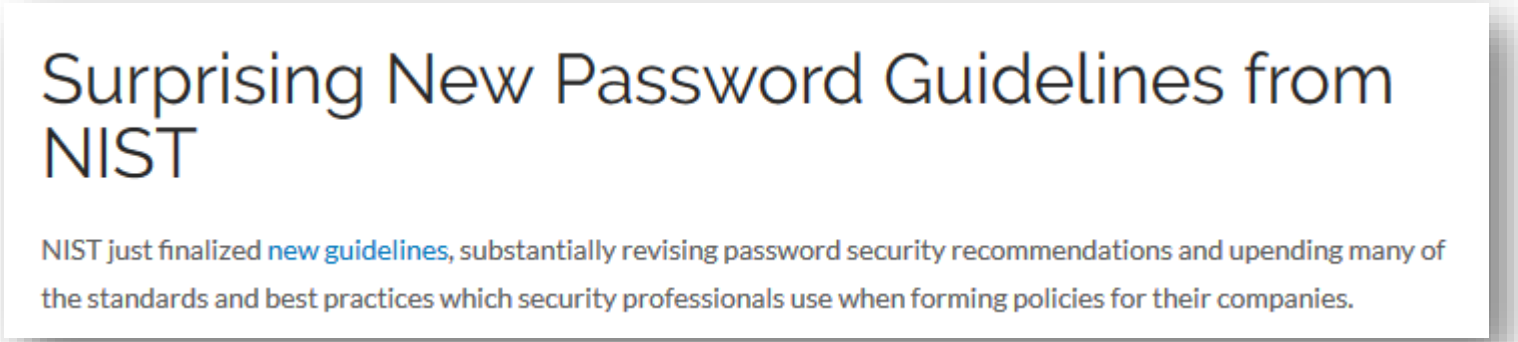
Whitelisting de Portas de Serviço

- Para servidores, estações de operação e outros equipamentos, recomenda-se o uso de firewall de host (ex: Windows Firewall) como medida complementar ao firewall de rede
- Para equipamentos de rede (ex: switches, routers) recomenda-se o uso de ACLs (Access Control Lists) em camada 2, 3 e 4
- Algumas referências:
  - NERC/CIP-007-6
  - IEC 62443-3-1
  - IEC 62351-10

Utilização de senhas fortes

- Utilize senhas fortes para usuários e contas de serviço, com altos padrões de complexidade
- Algumas referências:
  - NERC/CIP-007-6
  - IEC 62443-3-3
  - IEC 62351-7

Nova orientação do NIST



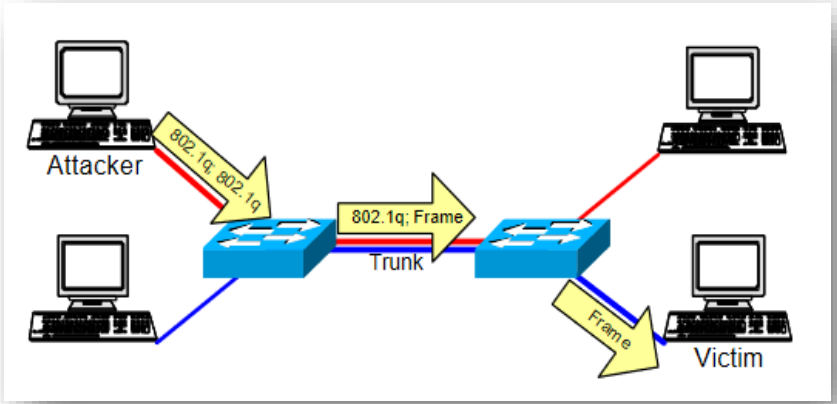
Surprising New Password Guidelines from NIST

NIST just finalized new guidelines, substantially revising password security recommendations and upending many of the standards and best practices which security professionals use when forming policies for their companies.

- Remover requisitos de expiração periódica de senhas
- Não use senhas complexas, use frases (passphrases)
- Todas as senhas cadastradas devem passar por um processo de verificação contra listas de senhas mais comuns ou capturadas (prevenindo ataques do tipo dicionário)

Segmentação de Tráfego

- O uso de VLANs limita domínios de broadcast e, portanto, reduz a superfície de ataque em caso de invasão
- Sempre use VLANs em configuração 1:1 (ou seja, 1 VLAN a 1 subrede)
- Defina e configure VLANs, inclusive a nativa. Isso evita ataques do tipo **Double Tagging**
- Algumas referências:
  - IEC 62443-3-1
  - IEC 62351-10

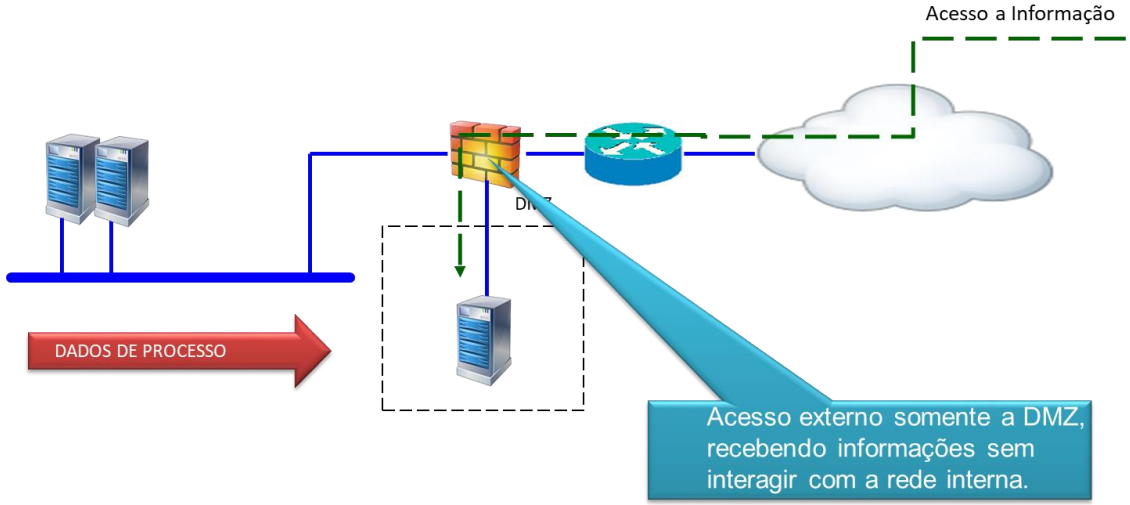


Gerenciamento de Ativos de Rede

- *"Em 2015 foram identificados **115.000** equipamentos de rede com firmware desatualizado. Destes, aproximadamente **106.000** (**92,2%**) possuem vulnerabilidades conhecidas"* [Cisco Annual Security Report 2016]
- Atualização regular de firmware para equipamentos de rede são recomendados
- Algumas referências:
  - IEC 62443-2-4
  - IEC 62351-10
  - NERC/CIP-007-6

Segurança do Perímetro de Rede

- Todas as informações que serão disponibilizadas a redes externas devem ser via DMZ
- A área de DMZ deve estar contida em uma sub-rede diferente das redes conectadas
- Algumas referências:
  - NERC/CIP-005-5
  - IEC 62443-3-1
  - IEC 62351-10



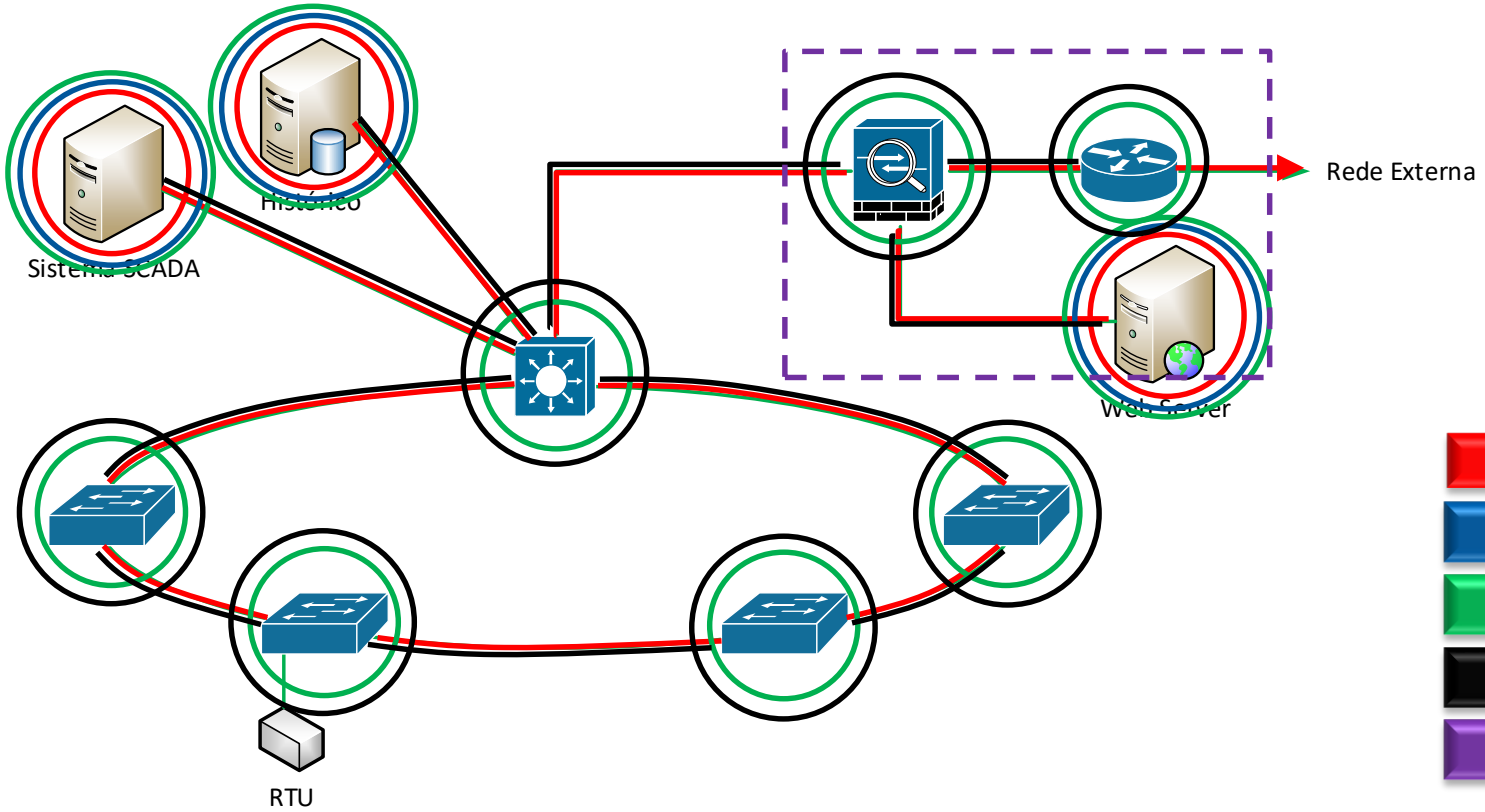
Mecanismos de Defesa Física

- Controle de Acesso às instalações
- Uso de método multi-fator de autenticação como, por exemplo, Cartão de Acesso + Identificação Visual
- Monitoramento das instalações por vídeo
- Procedimentos de visita acompanhada
- Controle de acesso a servidores, equipamentos de rede ou quaisquer outros equipamentos da sua infraestrutura
- Alarmes/Notificações em caso de intervenções indevidas em dispositivos como, por exemplo, desligamento, reinicialização, desconexão ou uso de dispositivos removíveis

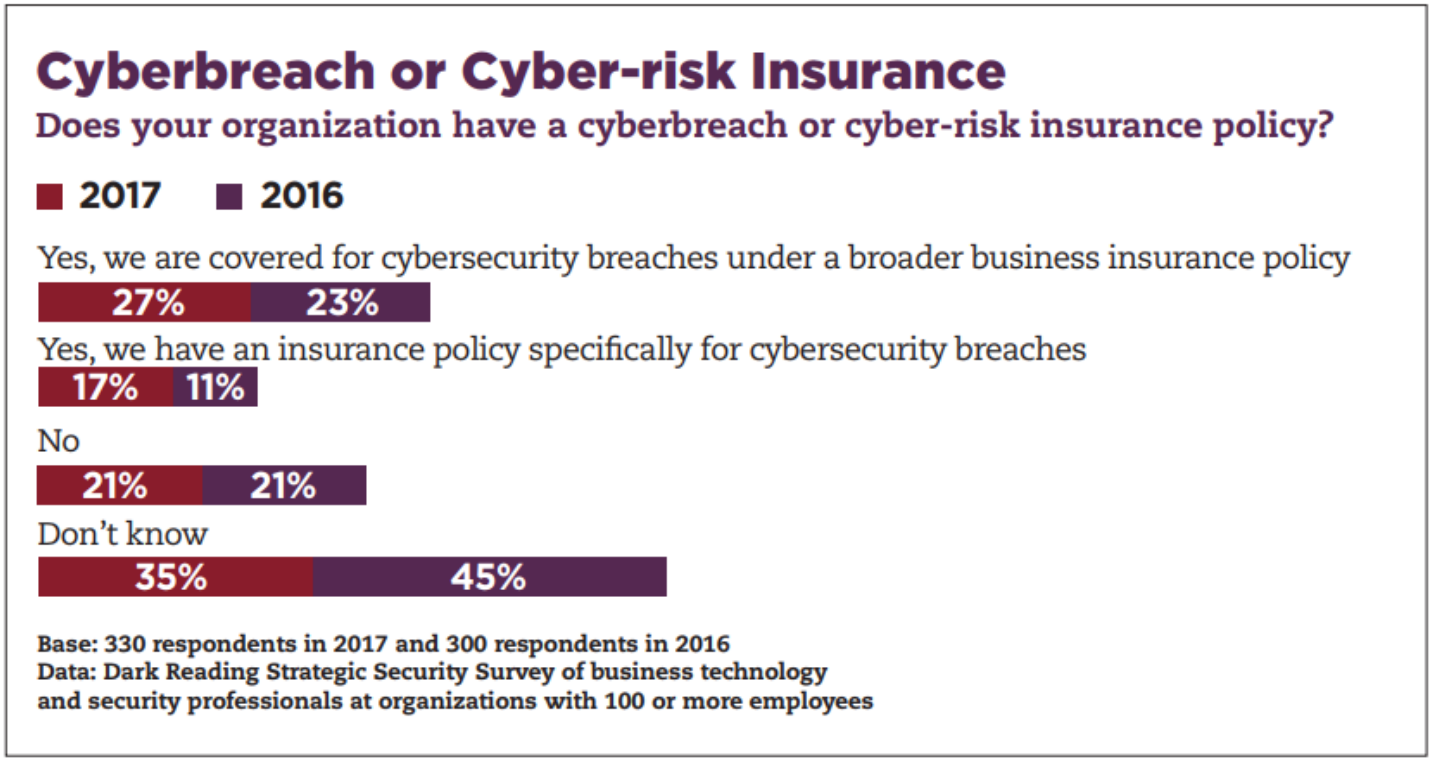
Políticas e Procedimentos

- Plano de Resposta a Incidentes
- Plano de Recuperação de Desastres
- Mecanismos de Controle de Modificações (Change Management)
  - Documentação de Rede (desenhos, endereços, hostnames) auditados e atualizados regularmente
  - Gerenciamento de Ativos: *"Você não pode proteger o que não conhece"*
- Treinamento e reforço anual de políticas de Segurança Cibernética (incluindo possíveis sanções em caso de descumprimento)
- Realização de Pen-Tests para avaliação de vulnerabilidades
- Patch Management – Redução do TTP (Time-to-Patch) por meio do uso de ambientes de teste de atualizações

Defesa em Profundidade Aplicada



Tendências



Para onde estamos indo?

- A Gartner prevê que em 2018, os investimentos em Segurança Cibernética chegarão a marca de USD 93 bilhões.
  - Marcos regulatórios reforçados como, por exemplo, o GDPR (General Data Protection Regulation)
  - Consciência da grande quantidade de ameaças que surgem diariamente
  - Digitalização como evolução do modelo de negócio atual
- Ainda de acordo com a Gartner o grande motor para a próxima geração na área de segurança cibernética serão os “ecossistemas digitais”: Diversos ambientes digitais que interagem entre si, incluindo o mundo IoT.

E no Brasil?

- Aumento de investimentos em Segurança Cibernética serão necessários também
  - Novos marcos regulatórios do setor elétrico: Revisão dos procedimentos de rede do ONS incluindo mecanismos de Segurança Cibernética
  - Novo marco legal do setor elétrico: Com o novo modelo do setor elétrico em discussão, a migração para sistemas cada vez mais integrados e digitalizados serão necessários para manter a produtividade e a eficiência das corporações. Isso cria um efeito colateral em Segurança Cibernética

OSIsoft.

Power Forum

BRASIL

2018

INFORMAÇÕES EM BREVE

Muito Obrigado!

Para fazer perguntas, utilize o painel
do lado direito, opção ‘chat’

OSIsoft®

Luiz Kawafune

lkawafune@osisoft.com

Sr Product Support Engineer

Latin America Cyber Security Champion

OSIsoft, LLC