FIEE Smart Future

FIEE Smart Energy

abinee 2019 TEC

Ilhas Temáticas

Segurança Cibernética para os Negócios e Cidades Inteligentes

TECNOLOGIA E SUSTENTABILIDADE

Prof. Josmar Giovannini - Conformidados

www.conformidados.com.br

Engenheiro eletricista pós graduado na área de administração de negócios;

Gestão de Controles Internos
Compliance
Riscos

Gestão Documental (+ 6 anos)

Líder do Comitê de Proteção de Dados da ABPRH: Associação Brasileira dos Profissionais de Recursos Humanos

Membro da High Technology Crime Investigation Association – HTCIA

Membro - Grupo de Estudos de Direito Digital e Compliance da FIESP

Membro - Comissão de Direitos Digitais e Compliance da OAB SP

Professor convidado do curso de formação de DPOs – FGV - Rio de Janeiro

Professor convidado – Curso MBA e Extensão (Direito, Direito Digital e Administração): Universidade Mackenzie, Anhembi-Morumbi/ Future Law

Professor licenciado da Universidade Paulista – UNIP;

Autor e coautor na área de gestão de dados pessoais e privacidade;

CIDADES INTELIGENTES

Geradoras e altamente dependente de dados para realização de estimativas, políticas e tomada de decisões

Alta capacidade de processamento e armazenamento de dados

Agregam dados e tecnologias para a sustentabilidade, bem-estar e desenvolvimento econômico dos seus habitantes

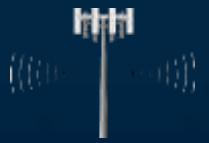
Utilização massiva de sensores, gerando dados em tempo real

IoT / Cloud / IA / ML

Exemplos de utilização massiva de tecnologia – Administração Pública

CONTROLE DE TRÁFEGO INTELIGENTE

CONTROLE DE ILUMINAÇÃO INTELIGENTE



APLICAÇÕES MÓVEIS

SISTEMAS DE GESTÃO DA CIDADE

TRANSPORTE PÚBLICO INTELIGENTE

SOLUÇÕES CLOUD E SAAS

CÂMERAS

DADOS PÚBLICOS

SERVIÇOS BASEADOS EM LOCALIZAÇÃO

SENSORES

MÍDIAS SOCIAIS

Exemplo Brasileiro

Câmeras de vigilância

Sensores de detecção de inundação e pluviômetro

Centro de Operações do Rio (FOR)

Dados Abertos (data.rio)

Iluminação de rua inteligente

Sistemas baseados em GPS

Sistema de controle climático

Sistema de controle de sinal de tráfego


DADOS
SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO
+
SEGURANÇA CIBERNÉTICA
→ **FUNDAMENTAIS**

Alta responsabilidade – Tratamento de dados
(impacto é diretamente proporcional ao volume tratado)

Cidades Inteligentes – Alvo de Ataques Cibernéticos

- Adoção de novas tecnologias (pontos adicionais de vulnerabilidades de segurança cibernética não exaustivamente testados)
- Segurança Fraca
- Atualização de patches (com delay devido ao fabricante ou negligenciada)
- Grande número de serviços dependendo de tecnologia => Grande superfície de ataque
- Criptografia: Falta de adoção de forma massiva
- Grande utilização – Tecnologia Wireless (mais fácil de ser atacada)
- Setor Público:
  - Orçamento, Treinamento e Recursos inadequados/insuficientes
  - Burocracia
  - Ausência de planos de resposta a incidentes eficientes

Exemplos – Consequência de ataques a cidades inteligentes

CONTROLE DE TRÁFEGO INTELIGENTE - Os dispositivos foram encontrados sem criptografar as comunicações, permitindo que os invasores alterassem os semáforos.

CONTROLE DE ILUMINAÇÃO INTELIGENTE - Os hackers mal-intencionados podem comprometer a iluminação pública de uma cidade e ativá-las à vontade. É possível escurecer grandes áreas da cidade, manipulando medidores inteligentes, explorando vulnerabilidades de segurança cibernética.

SISTEMAS DE GESTÃO DA CIDADE - Os sistemas de gestão da cidade podem ser invadidos e os dados criptografados por ransomware, sendo as autoridades extorquidas a pagar um resgate para recuperar os dados.

TRANSPORTE PÚBLICO INTELIGENTE - Ataques cibernéticos podem exibir informações incorretas nos sistemas de transporte público, podendo influenciar o comportamento das pessoas para causar atrasos e superlotação.

CÂMERAS - Câmeras de tráfego e de vigilância são os olhos da cidade e, ao cortá-las, os invasores podem cegar as cidades.

DADOS PÚBLICOS - Esses dados podem ajudar os invasores a determinar o melhor momento para ataques, agendar ataques, criar acionadores de ataques, coordenar ataques e assim por diante.

Exemplos – Consequência de ataques a cidades inteligentes

SENSORES - Sensores inteligentes podem ser hackeados para enviar dados falsos para sistemas que afetam a tomada de decisões. Hackers podem fingir terremotos, quebra de túneis ou pontes, inundações, etc, aumentando os alarmes e causando pânico geral.

MÍDIAS SOCIAIS: Pode ser usado como uma plataforma de amplificação para ataques MALICIOSOS. Por exemplo, os invasores podem aumentar o impacto de um ataque causando pânico em uma população promovendo ataques

APLICAÇÕES MÓVEIS - A invasão de aplicativos para dispositivos móveis tem impacto direto no comportamento dos cidadãos, já que eles tomam decisões com base no que os aplicativos para celular exibem.

SERVIÇOS BASEADOS EM LOCALIZAÇÃO - A falsificação por GPS e outros ataques são possíveis. Os sistemas obtêm informações de localização em tempo real e, se o local estiver errado, as decisões serão baseadas em informações incorretas.

SOLUÇÕES CLOUD E SAAS - Os servidores da cidade e a infraestrutura da nuvem estão expostos a ataques DDoS (Distributed Denial of Services) comuns que tornam os serviços inoperáveis.

Série de ataques cibernéticos sofridos recentemente por cidades inteligentes, comprometendo as suas infraestruturas inteligentes e pondo em risco a continuidade dos seus serviços.

23/12/2015: Ataques de rede elétrica na Ucrânia comprometeram três sistemas de empresas de distribuição de energia, afetando 30 subestações e deixando 230 mil pessoas sem eletricidade;

16/03/2016: Kemuri Water Company - Os invasores alteraram os níveis de produtos químicos usados para tratar a água e os dados de 2,5 milhões de clientes de serviços públicos ficaram comprometidos;

25/11/2016: Ferrovia Municipal de São Francisco . Ataque de ransomware em sistemas;

10/07/2017: Hackers de Dallas ativaram 156 sirenes de emergência por volta da meia-noite, levando a um caos público e a milhares de chamadas para o número de emergência 911;

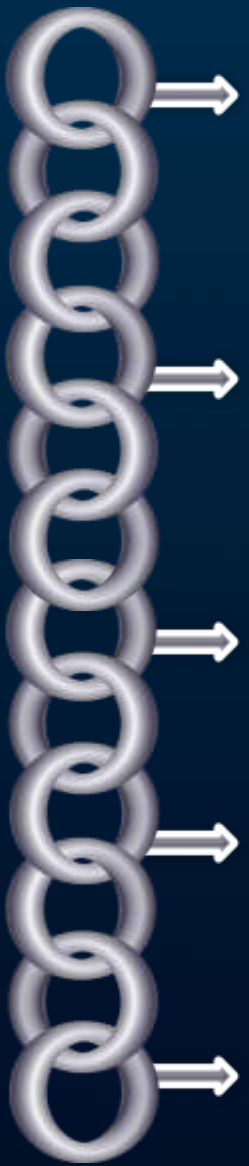
0/11/2017: Sistemas de Administração de Transportes da Suécia - Distributed Denial of Service (DDoS) do sistema afetado para monitorar trens, tráfego rodoviário levando ao caos de tráfego e atrasos;

18/11/2017: Sistemas de Trânsito Regional Sacramento: Ataque de ransomware eliminado 30 milhões de arquivos;

22/03/2018: Ataque do Atlanta Municipal Systems Ransomware aos sistemas da cidade, levando à paralisação dos vários sistemas da cidade.;

01/07/2018: Departamento de Segurança Interna, EUA: Hackers russos comprometeram as redes de várias concessionárias elétricas dos EUA e quase geraram blecautes;

O que se esperar da Administração Pública – Segurança de Cidades Inteligentes



Manutenção do foco na segurança cibernética, segurança da informação e na gestão do mundo virtual, a fim de melhorar a qualidade de vida dos seus habitantes pela melhora dos serviços públicos prestados

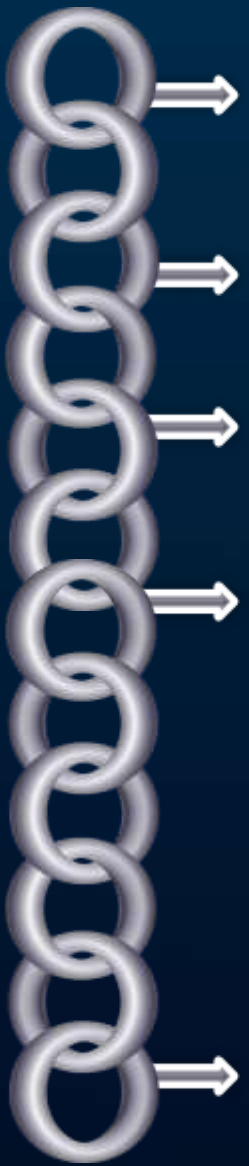
Garantia do direito fundamental da privacidade dos habitantes das cidades inteligentes, bem como dos seus dados pessoais,

Grande preocupação em Cidades Inteligentes pelo volume de dados pessoais tratados → *Imperativo o foco na gestão individual dos dados pessoais dos habitantes em cada uma das fases do ciclo de vida dos dados pessoais na administração pública*

Princípios de privacidade por projeto e por padrão devem ser incorporados na prática

O acesso aos dados tratados deve ser limitado estritamente aos atores devidamente treinados e informados quanto as suas responsabilidades e consequências sobre eventuais episódios de violação de segurança

Revisão dos contratos com prestadores de serviço (internet e telecomunicações), os quais deverão implantar e garantir a eficácia em processos de auditoria dos dados que tratam, garantindo as suas confidencialidades, integridades e disponibilidades



Gestão de crise adequada, visando a retomada da normalidade dos processos afetados por eventuais episódios de violação de segurança, identificação da profundidade e extensão dos prejuízos causados

Ações educativas para aumentar a conscientização dos usuários

Utilização de recursos forenses

Cidades Inteligentes crescem → *Infraestrutura se torna mais interconectada* → *Riscos se multiplicam*

Anonimização e criptografia são necessárias para dados em trânsito

Utilização de inteligência infiltrada para o desenvolvimento de defesas adequadas

Comunicação eficiente

O B R I G A D O

Josmar Lenine Giovannini Junior
Conformidados
josmar.giovannini@conformidados.com.br
www.conformidados.com.br
(11) 9 8620-3898