Como Proteger Sem Parar?

AVISO IMPORTANTE

O conteúdo técnico da palestra é de responsabilidade da empresa palestrante.

Fique à vontade para baixar o arquivo em PDF e se atualizar com as novas tecnologias apresentadas nesta edição.

Qualquer dúvida em relação ao conteúdo apresentado, você pode entrar em contato direto com o palestrante.

Como Proteger Sem Parar? - Objetivo

BAUMIER Autom@tion

- É realmente necessário parar?
- Quais os desafios que temos?
- Como implementar segurança de forma prática?

Quais são os riscos?

BAUMIER
Autom@tion

Interrupção na produção – Quanto vale sua hora parada?

BAUMIER Autom@tion

- Lucros cessantes
- Parar sua planta por 10 horas
- Degradação da matéria prima

Co

- In
- N
- Se

BLOG

O ataque ao oleoduto Colonial: o que aprendemos e o que fizemos nos últimos dois anos.

Lançado: 07 de maio d

Jen Easterly, Diretora d

Tom Fanning, Presiden

TÓPICOS RELACIONADOS: C
CRÍTICAS

Hoje faz dois anos desde
estampou manchetes em
enchendo seus carros cor
altamente conectada se t

Reuters

Mundo Negócios Mercados Sustentabilidade Jurídico Comentário Tecnologia Investigações Mais

500.000 a US$ 10 milhões, dependendo da apólice. Em seguida, o seguro entra em ação para cobrir o resgate, que no caso da Colonial foi de US$ 4,4 milhões, conforme declarou seu diretor executivo ao Wall Street Journal.

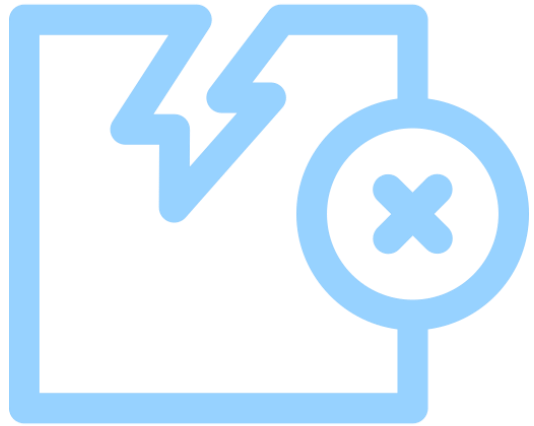
O seguro também cobre os custos de interrupção dos negócios e os custos dos parceiros da cadeia de suprimentos após um período de espera de oito a 24 horas.

A Colonial, que transporta cerca de 2,5 milhões de barris de combustível por dia, pode ter perdido entre US$ 9 milhões e US$ 15 milhões em receita devido à interrupção de seis dias, dependendo do período de espera, segundo cálculos da Reuters. A Colonial não comentou sobre suas perdas.

A boa notícia é que, desde esse evento, o governo Biden-Harris fez progressos significativos em nossa defesa cibernética coletiva, aproveitando todo o poder do governo dos EUA para lidar com todo o espectro da ameaça. Na Agência de Segurança Cibernética e de Infraestrutura (CISA), temos nos concentrado intensamente em aprimorar a resiliência em toda a infraestrutura crítica de nossa nação. Reconhecendo que as organizações precisam de uma maneira simples de acessar informações de segurança cibernética práticas e oportunas, desenvolvemos o stopransomware.gov para fornecer um local centralizado para alertas e orientações para empresas e indivíduos. Reconhecendo que somente uma colaboração coesa em todo o governo será capaz de enfrentar a ameaça em larga escala, lançamos a Força-Tarefa Conjunta de Ransomware com nossos parceiros do FBI para orquestrar a resposta do governo federal à epidemia de ransomware. Reconhecendo a necessidade de reunir a indústria, o governo e parceiros internos, e de eliminar as barreiras que criam brechas para o adversário, estabelecemos a Joint Cyber Defense Collaborative (JCDC) — um conceito que surgiu da Comissão Solarium do Ciberespaço dos EUA, da qual um de nós foi comissário — para catalisar uma comunidade de especialistas na linha de frente da defesa cibernética — dos setores público e privado — para compartilhar ideias e informações em tempo real, a fim de compreender as ameaças e reduzir os riscos para o país.

Danos a equipamentos – Como um malware pode danificar?

- Ataques focados ao dano
- Consequência como dano



Stuxnet Urâ nal

- O Stuxnet focou
- Aumentou a velc
- Parou abruptam

Jonathan Fildes
Repórter de tecnologia da BBC News

23 setembro 2010

Um tipo de vírus de computador, dos mais sofisticados já detectados, pode ter como alvo infraestrutura iraniana de "alto valor", segundo especialistas ouvidos pela BBC.

A complexidade do malware Stuxnet, programa que permite o acesso remoto ao computador infectado, sugere que ele deve ter sido criado por algum governo nacional, de acordo com alguns analistas.

Acredita-se que o vírus seja o primeiro especialmente criado para atacar infraestruturas reais, como usinas hidroelétricas e fábricas.

Um pesquisa da Symantec, empresa americana de segurança informática, sugere que quase 60% de todas as infecções mundiais ocorrem no Irã.

"O fato de que vemos mais infecções no Irã do que em qualquer outro lugar do mundo nos faz pensar que o país era alvo", diz Liam O'Murchu, da Symantec.

O Stuxnet foi detectado por uma empresa de segurança de Belarus em junho, embora esteja circulando desde 2009 e vem sendo intensivamente estudado desde então.

Máquinas

O Stuxnet, ao contrário da maioria de viroses, não está conectado com a internet. Ele infecta máquinas Windows por meio de portas USB e pen drives usados para transportar arquivos.

Segurança Operacional – Quanto vale uma vida?

BAUMIER Autom@tion

- Mecânico
- Biológico
- Químico

ETA de

- Acesso
- Uso de
- Nível r
- Funcio

INDUSTRIAL DEFENDER®

Cibersegurança de OT | Água e Esgoto

Estação de tratamento de água da Flórida sofre ataque cibernético.

Steve Kardon

10 de abril de 2023

Na sexta-feira, 5 de fevereiro de 2021, um hacker iniciou um ataque a uma estação de tratamento de água em Oldsmar, Flórida, que alterou brevemente os níveis de hidróxido de sódio de 100 partes por milhão para 11.100 partes por milhão. O ataque ocorreu a cerca de 24 quilômetros do local do Super Bowl, dois dias antes do evento. Se tivesse sido bem-sucedido, o ataque teria elevado a quantidade de hidróxido de sódio na água a um nível extremamente perigoso. Felizmente, um funcionário atento percebeu a tentativa de invasão e a impediu.

BAUMIER Autom@tion

Vazamento de dados – A importância da informação

BAUMIER Autom@tion

- Procedimentos interno
- Senhas de acesso
- Documentos sensíveis

AN

Sistemas da ANP seguem fora do ar após tentativa de ataque; agência não divulga preços de combustíveis

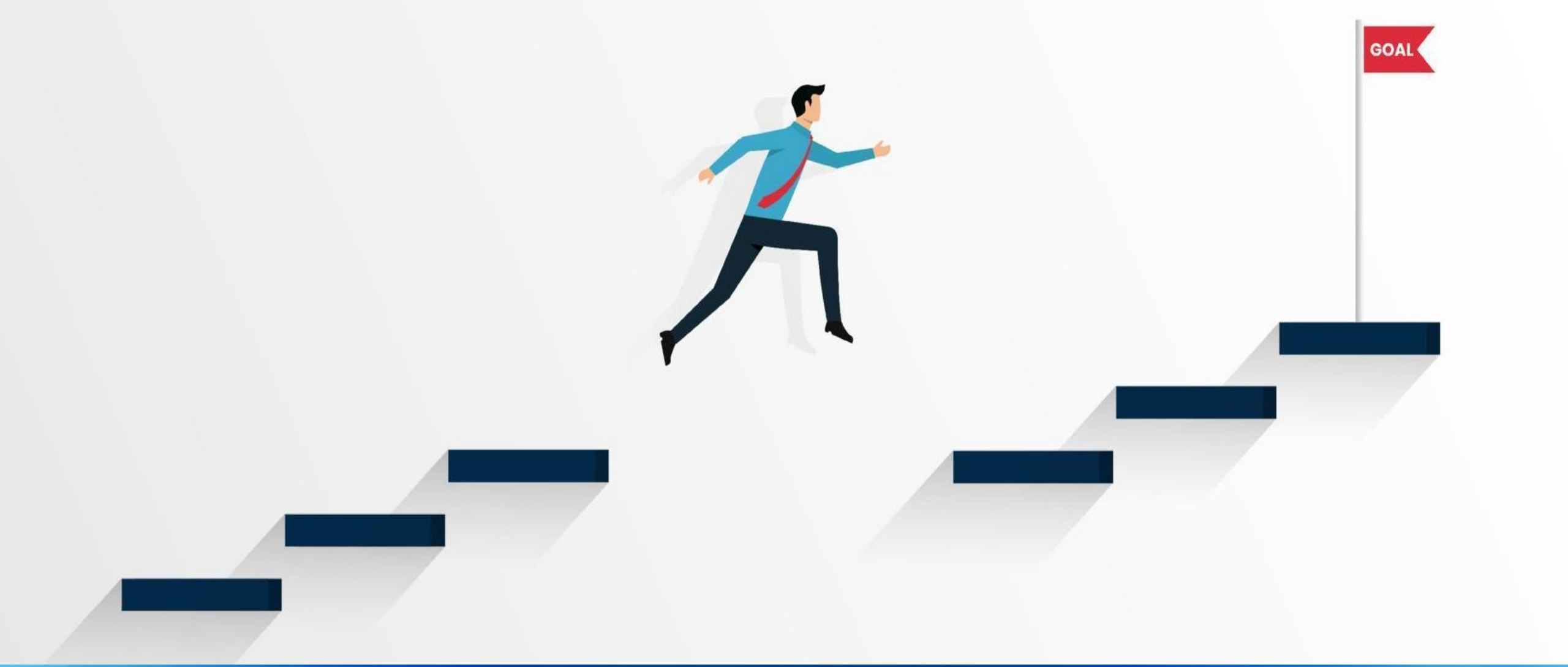
Em nota enviada na semana passada, a agência informou que os sistemas foram retirados do ar como medida de segurança, para avaliação dos riscos.

Nesta quinta-feira (11), a **ANP** disse em nota que segue "tomando todas as providências para o retorno dos seus sistemas o mais rápido possível". "O trabalho está sendo feito de forma criteriosa, para que a retomada ocorra com segurança", diz a nota.

Quais são os riscos?

BAUMIER
Autom@tion

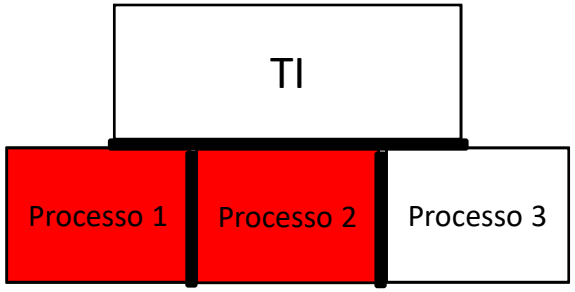
Desafios do Setor

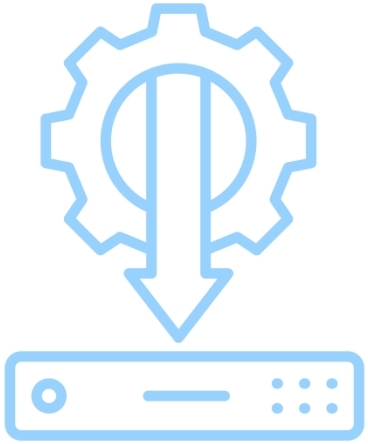


Sistemas Legados – Atualização da planta

BAUMIER Autom@tion

- Dispositivos desatualizados (Hardware e Software)
- Redes sem segregação
- Funções de segurança desabilitadas
- Ex: Switch

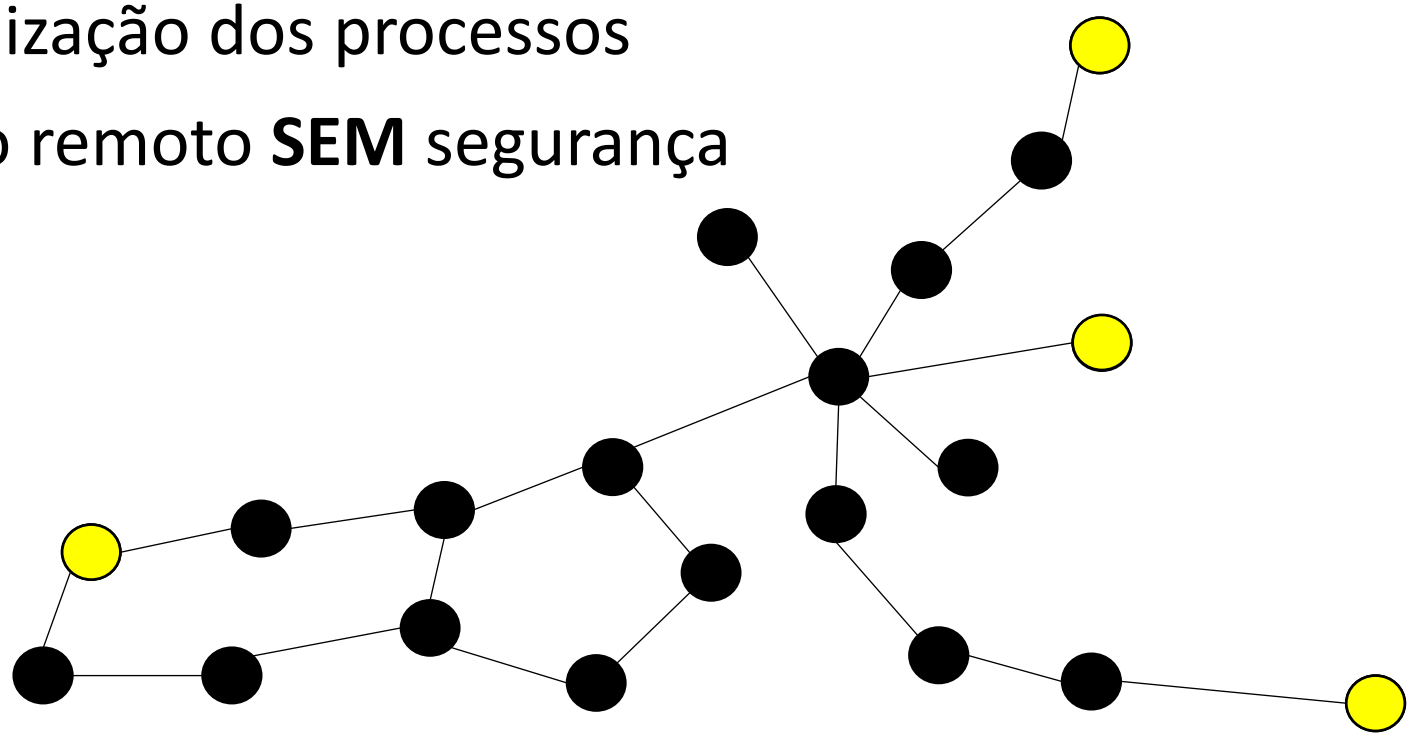




Superfície de Ataque – Conectividade sem consciência

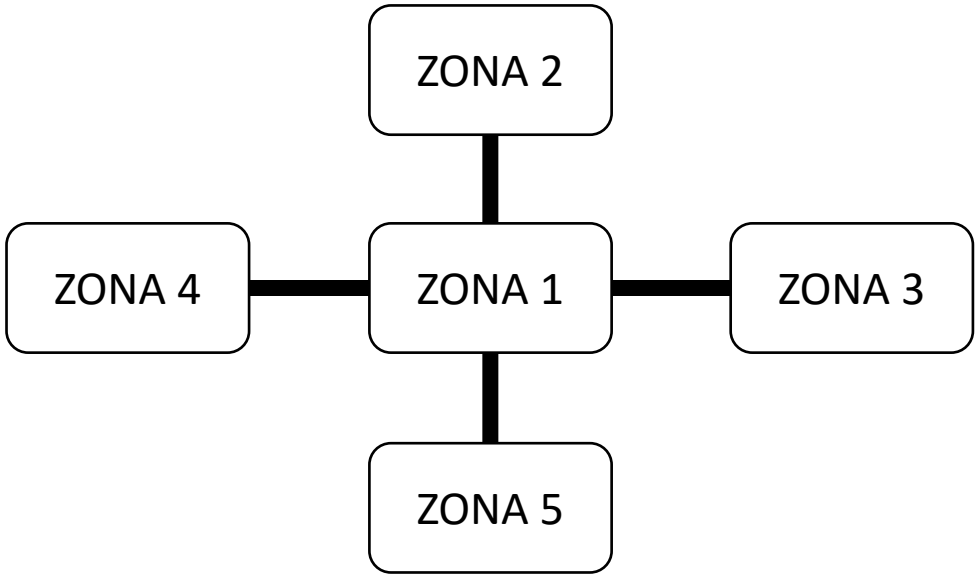
BAUMIER Autom@tion

- Expansão da planta
- Virtualização dos processos
- Acesso remoto **SEM** segurança



Padrões de Segurança – Quais normas que nos regulamenta?

- IEC 62443
- Zonas confiáveis
- Conduítes seguros



Desinformação – O pior de tudo...

BAUMIER Autom@tion

- Resumo de todos os problemas mostrados
- Como contornar?

Ameaça, Vulnerabilidade, Risco e Impacto

BAUMIER
Autom@tion

Ameaça

- Evento c
- Como m
- Conhece

STOP RANSOMWARE

RESOURCES | NEWSROOM | ALERTS | REPORT RANSOMWARE | CISA.GOV

Home / Stop Ransomware / Resources

Resources

- #StopRansomware Guide
- Bad Practices
- Campaigns
- Fact Sheets and Information
- Public Safety Emergency Communications Resources
- Ransomware 101
- Ransomware Vulnerability Warning Pilot
- Sector Risk Management Agencies
- Services
- Webinars

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent months, ransomware has dominated the headlines, but incidents among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations have been growing for years.

Malicious actors continue to adapt their ransomware tactics over time. Federal agencies remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world.

Have you been hit by ransomware? The Ransomware Response Checklist from the updated #StopRansomware Guide is your next stop.

Want to learn how to avoid ransomware? How Can I Protect Against Ransomware is a valuable resource to learn about avoiding Bad Practices.

The U.S. Secret Service provides guidance for how and where to report a cyber incident in their Preparing for a Cyber Incident document. Likewise, NIST's Ransomware Protection and Response provides information on response and recovery.

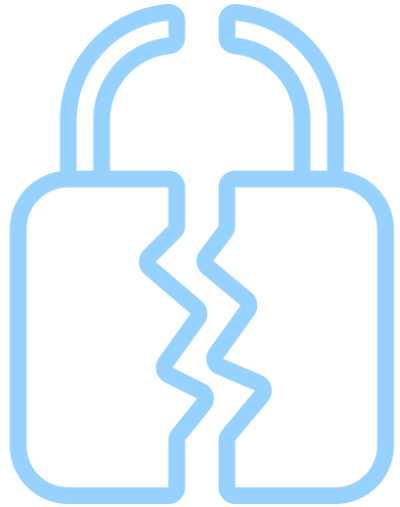
CISA and Australian Signals Directorate's Australian Cyber Security Centre (ACSC) published a Business Continuity in a Box which can help organizations with swiftly and securely standing up critical business communications and application functions during or following a cyber incident, whether ransomware or other method. Using this resource, organizations can maintain or re-establish the basic functions needed to operate a business while responding to the issues affecting their existing systems.

BAUMIER Autom@tion

Vulnerabilidade – O potencial ataque

BAUMIER Autom@tion

- Falha ou fraqueza exploráveis
- Como mitigar?
- Estudo da sua rede feita por um profissional de Cyber
- Implementação das boas práticas de segurança



Riscos – A chance de exploração

BAUMIER Autom@tion

- Falha ou fraqueza exploráveis
- Risco = ameaça + vulnerabilidade
- Como mitigar?
- Consultoria orientativa
- Testes controlados dos riscos

Impacto – O Dano Final

BAUMIER Autom@tion

- Consequência da exploração da vulnerabilidade
- Como mitigar?
- Preventivo
- Paliativo

Conclusão

Como Proteger Sem Parar? - Objetivo

- Não precisamos parar
- Quais os desafios, quais temos?
- Como implementar segurança de forma prática?

Referências

https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
https://www.cisa.gov/stopransomware/resources
https://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html
https://www.bbc.com/portuguese/noticias/2010/09/100923_iran_virus_rc
https://economia.uol.com.br/noticias/estadao-conteudo/2022/08/15/sistemas-da-anp-estao-ha-11-dias-fora-do-ar-e-sem-perspectiva-de-retorno.htm
https://g1.globo.com/economia/noticia/2022/08/12/sistemas-da-anp-seguem-fora-do-ar-apos-tentativa-de-ataque-agencia-nao-divulga-precos-de-combustiveis.ghtml
https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack
https://www.flaticon.com/br/icones-gratis/lei
https://www.reuters.com/technology/after-colonial-attack-energy-companies-rush-secure-cyber-insurance-2021-05-28/
https://cybermap.kaspersky.com/pt
https://threatmap.checkpoint.com/

Obrigado!

Nicolas Souza
Baumier Automation
Especialista de Redes
Nicolas Souza

contato@baumier.com.br
11 4332-3280