SEUS DADOS ESTÃO **SEGUROS?**

ESTUÁRIO TI

QUEM SOU EU

Felipe Maciel

Formação e MBA em Administração pela UPE.
Pós graduação em planejamento e controle empresarial pela FGV (RJ).
CEO e cofundador da Estuário TI há 13+ anos 🚀
Cibersegurança por amor e transformação digital por convicção 🔐
Paixão por unir inovação, eficiência e resultados 💻

QUEM SOMOS

A Estuário TI é uma empresa pernambucana especializada em Cibersegurança, oferecendo soluções personalizadas para proteção de dados em diversos setores como saúde, educação, direito e construção civil, voltada principalmente para o setor privado.

NOSSA HISTÓRIA

Fundada em 2012 no Recife, um dos maiores parques tecnológicos do Brasil, a Estuário integra o ecossistema da Cultura Digital pernambucana. Estamos sediados em Recife e contamos com uma filial em São Paulo.

O que é Ransomware?

Ransomware é um tipo de software malicioso que, uma vez instalado em um sistema, criptografa arquivos importantes e exige um pagamento, geralmente em criptomoedas, para sua descriptografia. Ele funciona como um "sequestro digital", impedindo o acesso aos dados até que o resgate seja pago.

Múltiplas Vias de Infecção

As infecções podem ocorrer por meio de phishing (e-mails maliciosos), exploração de vulnerabilidades em sistemas e softwares desatualizados, ou credenciais roubadas que permitem acesso indevido à rede.

Paralisação Total das Operações

O impacto vai além da perda de dados; o ransomware interrompe completamente as operações críticas de uma organização, resultando em perdas financeiras significativas e danos à reputação.

Panorama dos Tipos de Ransomware

Crypto-ransomware
Criptografa arquivos e exige resgate para a chave (ex: WannaCry, LockBit).

Double Extortion
Combina criptografia com a ameaça de vazar dados confidenciais publicamente, aumentando a pressão por pagamento.

Locker-ransomware
Bloqueia o acesso ao sistema operacional, impedindo que o usuário utilize o computador, mas sem criptografar arquivos específicos.

Ransomware-as-a-Service (RaaS)
Modelos de negócio onde cibercriminosos "alugam" infraestrutura e ferramentas de ransomware para outros atacantes, com divisão dos lucros.

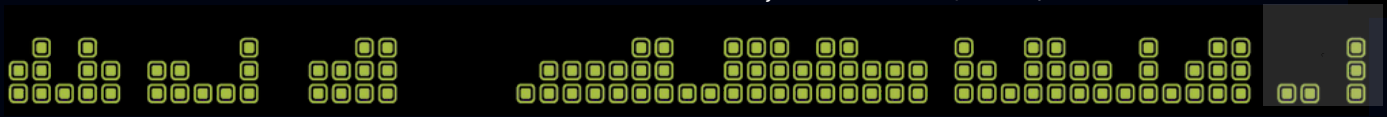
Caso Unicap: Um Estudo de Caso Real

Em 16 de julho de 2025, por volta das 05h40, a Universidade Católica de Pernambuco (Unicap) sofreu um ataque de ransomware que criptografou seus servidores críticos.
O incidente paralisou grande parte de suas operações digitais e impactou estudantes e funcionários.

- **Impacto e consequências:** O portal da universidade ficou inacessível, as matrículas foram prorrogadas, aulas e serviços administrativos precisaram ser adaptados para o formato remoto.

- **Repercussão:** O incidente gerou preocupação na comunidade acadêmica e serviu como um alerta sobre a criticidade da cibersegurança em instituições de ensino.

- **Transparência:** A Unicap comunicou em seu site e Instagram o ocorrido e formalizou uma queixa-crime na Delegacia de Repressão aos Crimes Cibernéticos de Pernambuco e comunicou o ocorrido à Autoridade Nacional de Proteção de Dados (ANPD).



Caso NYU: Um Estudo de Caso Real

Durante um período de cerca de três horas, o tráfego destinado ao site www.nyu.edu foi redirecionado para uma página que o invasor publicou no GitHub. O incidente de 22 de março na NYU parece estar relacionado ao mesmo agente envolvido em um incidente semelhante na universidade de Minnesota ocorrido há alguns anos. Não foi um caso de ransomware, mas sim de falha no sistema, como o próprio invasor confessou em postagem no X.

- **Impacto imediato:** exposição de dados de alunos com notas e gráficos para admissões que se diziam fora da lei. A universidade disse que os dados publicados eram falsos.
- **Resposta imediata:** consultoria em cibersegurança, restauração do tráfego e notificação às autoridades.
- **Transparência:** A NYU estabeleceu uma linha direta para receber e responder perguntas sobre o incidente.

https://www.nyu.edu/about/news

Lições Essenciais dos Casos

1. Backups são a Salvação
A existência de backups atualizados e isolados foi crucial para a recuperação de dados e a retomada das operações. Sem eles, o dano teria sido irreparável.

2. Resposta Rápida é Vital
A agilidade na detecção e no isolamento do ataque minimizou a propagação do ransomware e a extensão dos danos. Cada minuto conta.

3. Planos de Continuidade
Ter um Plano de Continuidade de Negócios e de Recuperação de Desastres (DR) bem definidos e testados é essencial para manter a instituição funcional durante uma crise.

4. Comunicação Transparente
Uma comunicação clara e constante com estudantes, funcionários e mídia foi fundamental para preservar a confiança e gerenciar a crise de imagem.

Por que os ataques cibernéticos são uma preocupação para universidades e faculdades?

Por uma série de razões:

- Valor → Alto custo e muitos dados pessoais.
- Baixa tolerância a interrupções → tornam-se mais propensas a pagar resgates para reduzir danos.
- Superfície de ataque ampla e complexa → com muitos dispositivos pessoais e IoT conectados, difíceis de proteger e cheios de pontos de entrada.
- Redes de parceiros e fornecedores complexas → aumentam o risco de violações de terceiros.
- Investimento concentrado em acesso e funcionalidade → a maior parte do orçamento de TI vai para facilitar o uso, e não para fortalecer a segurança.

Prevenção: Boas Práticas em Cibersegurança

- Política de Backups 3-2-1: Três cópias dos dados, em dois tipos de mídia diferentes, com uma cópia offsite.
- Atualizações e Patches: Mantenha sistemas e softwares sempre atualizados para corrigir vulnerabilidades conhecidas.
- Autenticação Multifator (MFA) ou 2FA: Adicione uma camada extra de segurança para todos os acessos.
- Segmentação de Rede: Divida a rede em zonas isoladas para limitar a propagação de ataques.
- Treinamento Contínuo: Capacite funcionários para reconhecer e evitar ameaças (ex: phishing).
- Monitoramento Proativo: Utilize ferramentas para detectar atividades suspeitas em tempo real.

Conclusão e Recomendações Finais

- **Ameaça Persistente**

O ransomware é uma realidade crescente, e nenhuma organização está imune.

- **Investimento em Prevenção**

Prevenir é sempre mais barato e menos disruptivo do que remediar um ataque.

- **Planejamento é Essencial**

O caso Unicap reitera a importância de planos robustos de resposta e backups seguros.

- **Responsabilidade Coletiva**

A cibersegurança é uma cultura que deve ser abraçada por todos na organização, não apenas pela TI.

MUITO OBRIGADO

/ ESTUARIO.TI • WWW.ESTUARIOTI.COM.BR

eBook

Navegue sem medo: seu escudo contra ameaças digitais

Aprenda, de forma simples e objetiva, como proteger seus dados, evitar golpes e navegar com mais segurança.

- ✅ Dicas práticas
- ✅ Explicações claras
- ✅ Glossário essencial

- contato@estuarioti.com.br
- felipe@estuarioti.com.br
- estuarioti.com.br
- @estuario.ti