

# Seminário II - Segurança em Sistemas de Informação

Aluno: Ramon Lopes de Queiroz

# Sumário:



- **1. Introdução:** ..... 3
- **2.1 Objetivo Geral:** ..... 4
- **2.2 Objetivo Específico:** ..... 5
- **3.1 Hacking:** ..... 6
- **3.2 Diferença de Ethical Hacker (Hacker) e Hacker (Cracker):** ..... 7
- **3.3 Hacktivismo Contra Israel:** ..... 8
- **4. Caso 1:** ..... 11
- **5. Caso 2:** ..... 17
- **6. Caso 3:** ..... 24
- **7. Conclusão:** ..... 29
- **8. Referências Bibliográficas:** ..... 30

# 1. Introdução:



A informação é um dos ativos mais valiosos para indivíduos e organizações. Desde dados pessoais e financeiros até segredos comerciais e estratégias de negócio, tudo circula e é armazenado em sistemas de informação. A segurança da informação deixou de ser um mero detalhe técnico para se tornar um pilar dos negócios, a proteção da privacidade e a manutenção da confiança de clientes e parceiros. Neste contexto, a análise de incidentes reais torna-se uma ferramenta indispensável para a compreensão das vulnerabilidades e para o desenvolvimento de estratégias de defesa mais eficazes.

## 2.1. Objetivo Geral:



Analisar três estudos de caso de cibersegurança de alto impacto ocorridos em Israel, com o propósito de identificar as falhas de segurança, avaliar os impactos gerados e verificar o que poderia ser feito para a prevenção e qual foi a resposta a incidentes.

## 2.2. Objetivo Específico:



Descrever o ataque à seguradora Chirbit, a paralisação do Hillel Yaffe Medical Center e o vazamento de dados do site Atráf, verificando como foram operados, identificar os prejuízos causados pelos incidentes, tanto socialmente quanto economicamente, examinar as consequências sofridas pelas vítimas e organizações, apontar as vulnerabilidades do sistema e a ausência de medidas preventivas, e a partir disso, tirar lições de cibersegurança, proteção de dados e segurança de infraestruturas.

## 3.1. Hacking:

Uso indevido de dispositivos como computadores, smartphones, tablets e redes para causar danos ou corromper sistemas, coletar informações, roubar dados e documentos ou interromper atividades relacionadas a dados.

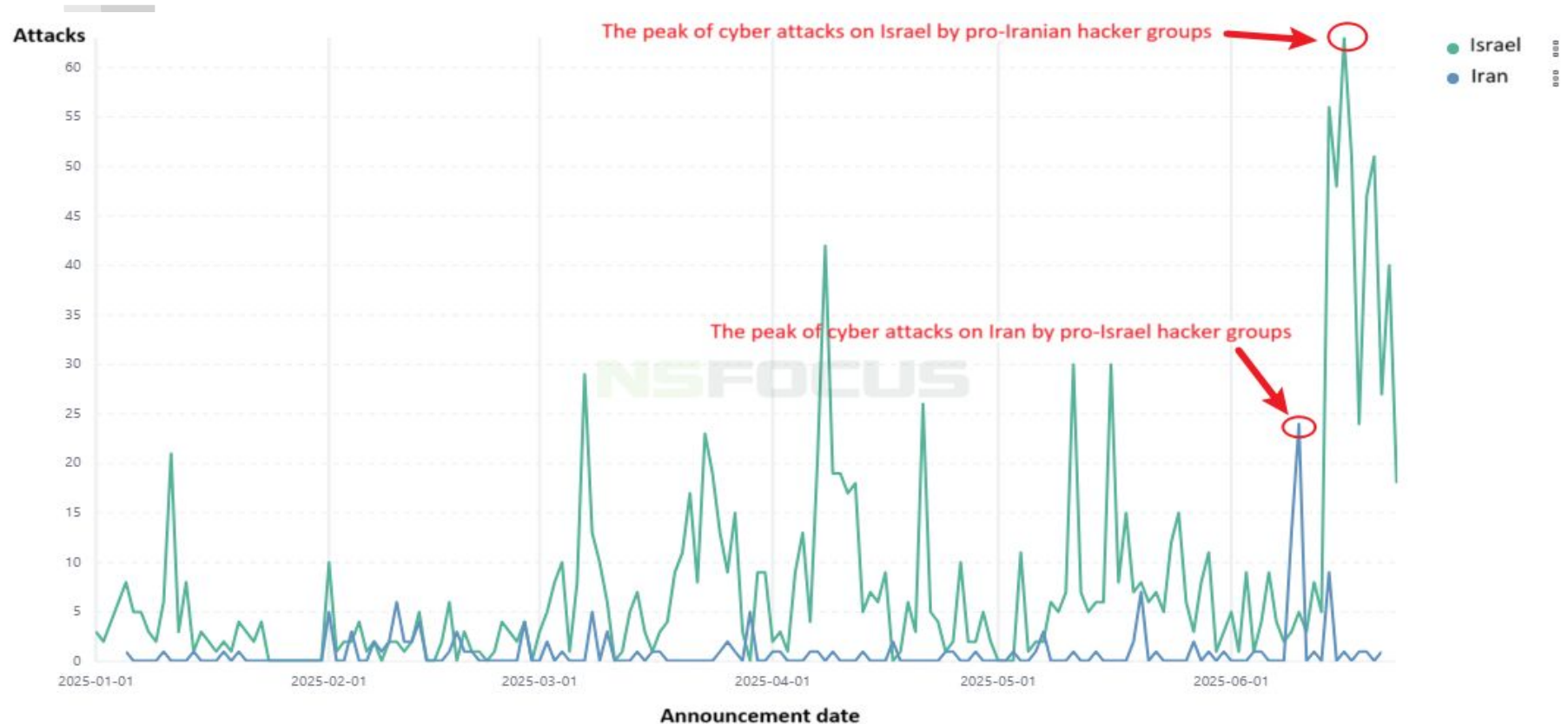
- **Tipos de hackers:**
  - White Hats
  - Black Hats
  - Grey Hats
- **Dispositivos mais vulneráveis:**
  - Webcams
  - Roteadores
  - Email
  - Telefones desbloqueados



## 3.2. Diferença de Ethical Hacker (Hacker) e Hacker (Cracker):

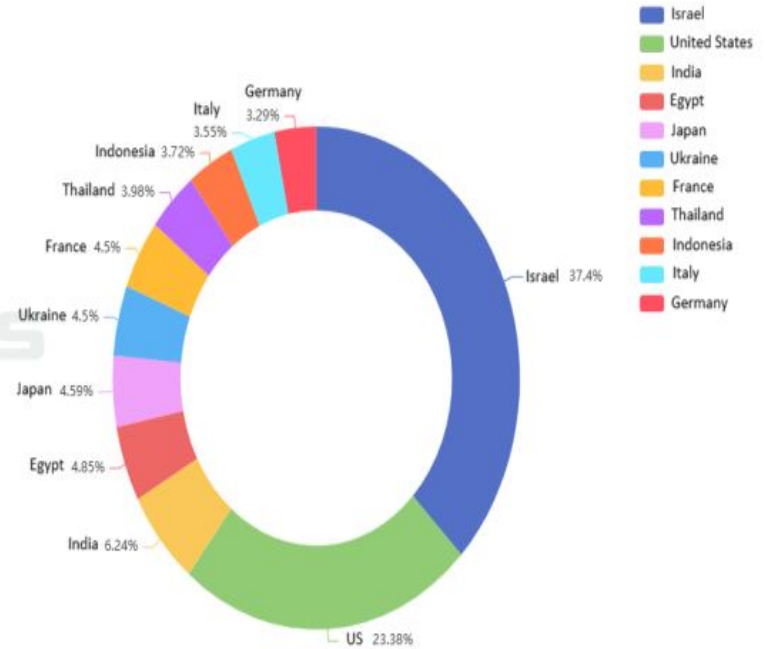
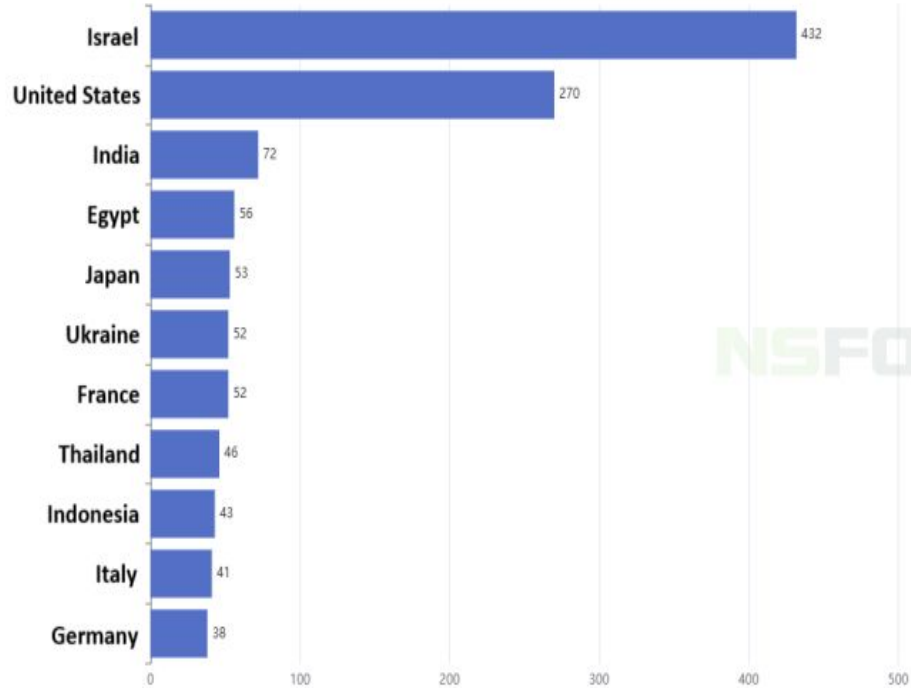


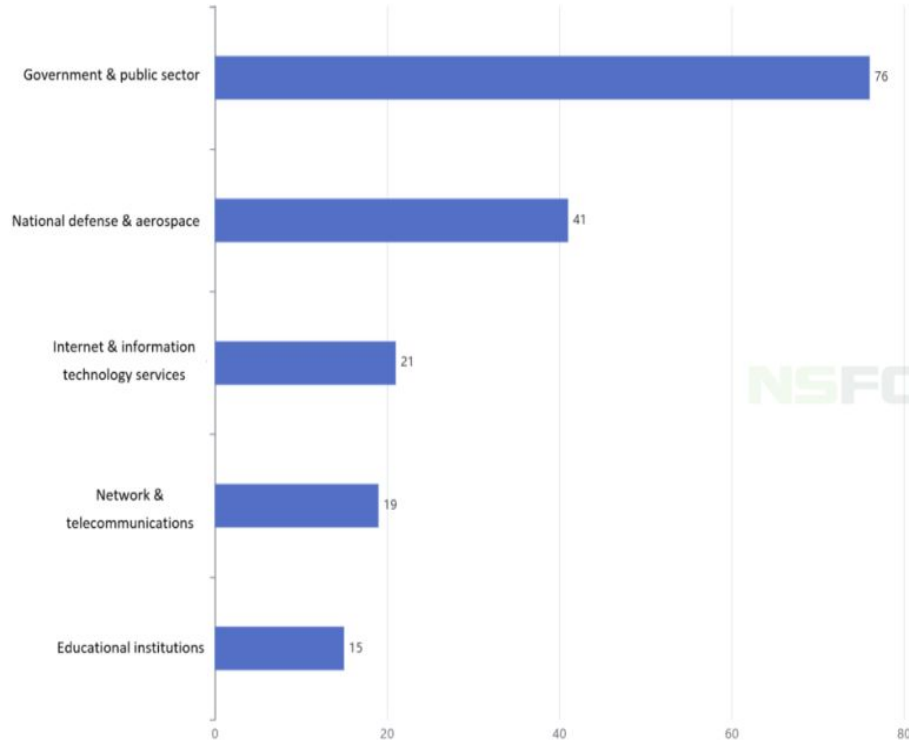
### 3.3. Hacktivismo contra Israel:



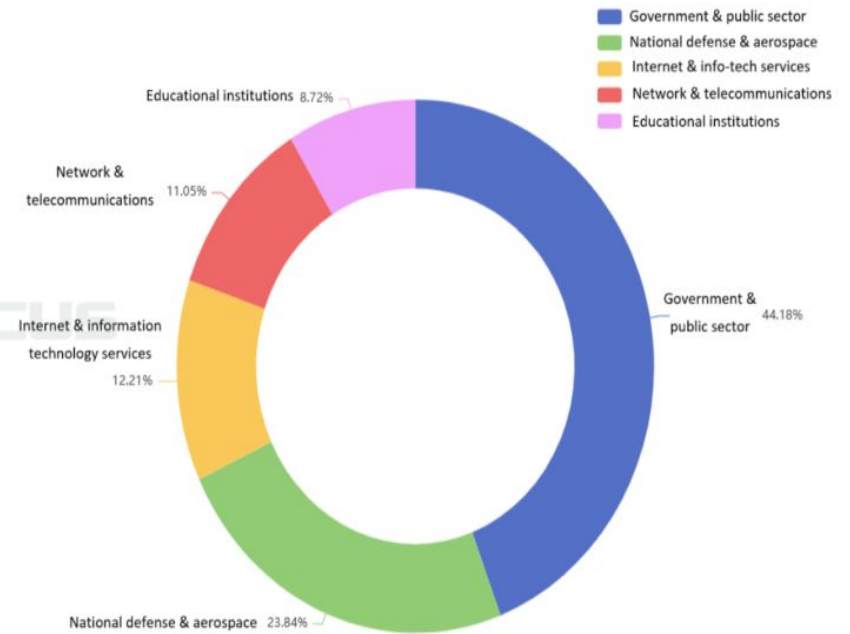


## Global hacker activities from June 13 to June 23





Top 5 industries attacked in Israel



## 4. Caso 1: O Ataque à Seguradora Shirbit (2020):



### 4.1. Descrição do Incidente:

- **Incidente:** Ataque massivo de *ransomware* em dezembro de 2020 à seguradora Shirbit, causado por um grupo de hackers chamados de “Black Shadow”.
- **Ação:** Roubo de grande volume de dados sensíveis de clientes, como documentos de identidade, registros médicos e informações de pagamento.
- **Extorsão:** O grupo exigiu um resgate de aproximadamente US\$ 1 milhão em Bitcoin.
- **Desfecho:** Com a recusa do pagamento, os invasores iniciaram o vazamento dos dados em lotes na internet, afetando inclusive funcionários do setor público e judiciário.

# Ataque por ransomware:



## 4.2. Prejuízos Causados:



### **Financeiros:**

- Custos elevados com investigação, remediação e fortalecimento da segurança.
- Perda de clientes e receita.
- Custos indiretos superaram o valor do resgate solicitado.

### **Sociais:**

- Geração de uma crise de confiança na segurança de infraestruturas críticas nacionais.
- Dano à imagem da empresa por falha na proteção de dados críticos.

## 4.3. Consequências:



### **Para as Vítimas:**

- Exposição a fraudes, roubo de identidade e chantagem.
- Constrangimento pela divulgação de informações privadas.

### **Para a Organização:**

- Investigação rigorosa por órgãos reguladores.
- Responsabilização por negligência, resultando em sanções e risco de ações judiciais coletivas.
- Reputação foi manchada tanto para os clientes quanto para o governo;

## 4.4. Falhas de Segurança Existentes:



A investigação revelou a ausência de controles de segurança básicos:

- Inexistência de um Diretor de Segurança da Informação (CISO) em tempo integral.
- Utilização de senhas fracas em sistemas críticos.
- Não implementação de autenticação de dois fatores (2FA).
- Falta de segmentação de rede, o que facilitou o movimento lateral dos invasores após o acesso inicial.

## 4.5. Ações Corretivas:



- Implementação de um plano de recuperação.
- Contratação de especialistas em cibersegurança para investigação.
- Reconstrução da infraestrutura de TI com protocolos de segurança mais rígidos.
- Melhoria dos sistemas de monitoramento e resposta a incidentes.



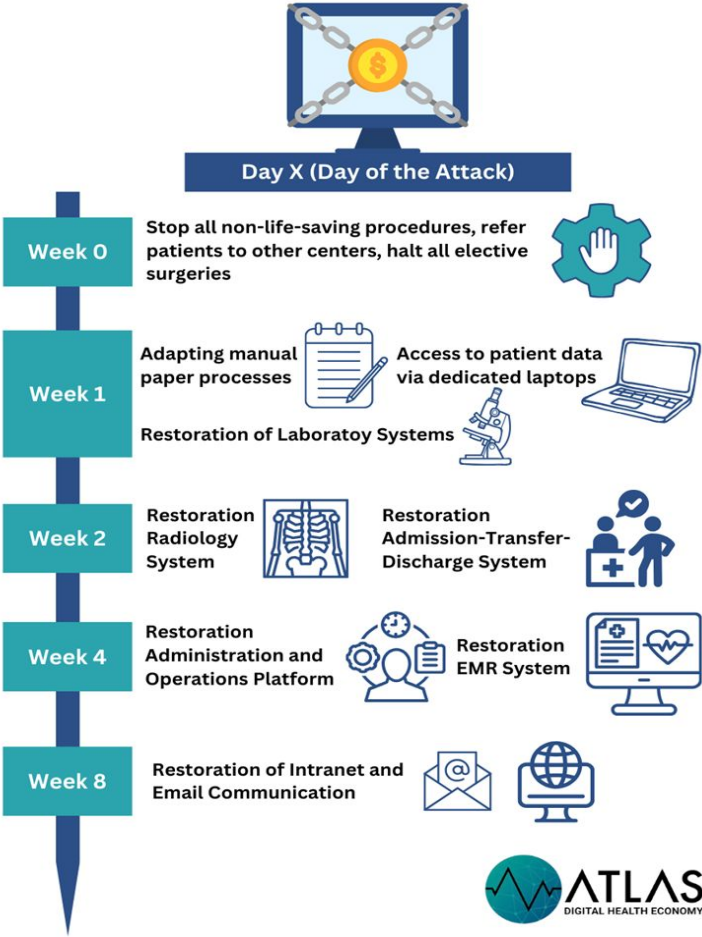
## 5. Caso 2: Ataque ao Hillel Yaffe Medical Center (2021):



### 5.1. Descrição do Incidente:

- **Incidente:** Ataque de *ransomware* em outubro de 2021.
- **Impacto:** Paralisação completa dos sistemas de TI do hospital (cirurgias inclusive).
- **Ação:** Servidores e estações de trabalho foram criptografados.
- **Extorsão:** O grupo exigiu um resgate multimilionário.
- **Desfecho:** Com a ajuda do governo, o hospital conseguiu se recuperar e atualizar sua segurança. No entanto, levou um mês para recuperar os dados, nenhuma informação foi vazada, e nenhum equipamento médico vital foi afetado.

# Como Hospitais devem agir:



Steady Computer System Recovery



## 5.2. Prejuízos:



### **Prejuízos Operacionais:**

- Interrupção crítica de serviços de saúde.
- Cancelamento de cirurgias, transferência de pacientes e retorno a registros manuais em papel.

### **Prejuízos Financeiros e Sociais:**

- Custos elevados com recuperação e perda de receita.
- Pânico social e debate nacional sobre a vulnerabilidade do setor de saúde.

## 5.3. Consequências:



### **Para os Pacientes:**

- Tratamentos adiados e risco de agravamento de condições de saúde.
- Aumento do risco de erros médicos pela falta de acesso a prontuários.

### **Para a Organização:**

- O processo de recuperação levou semanas.
- O incidente motivou a exigência de padrões de segurança mais elevados para todo o setor de saúde em Israel.

## 5.4. Falhas de Segurança:



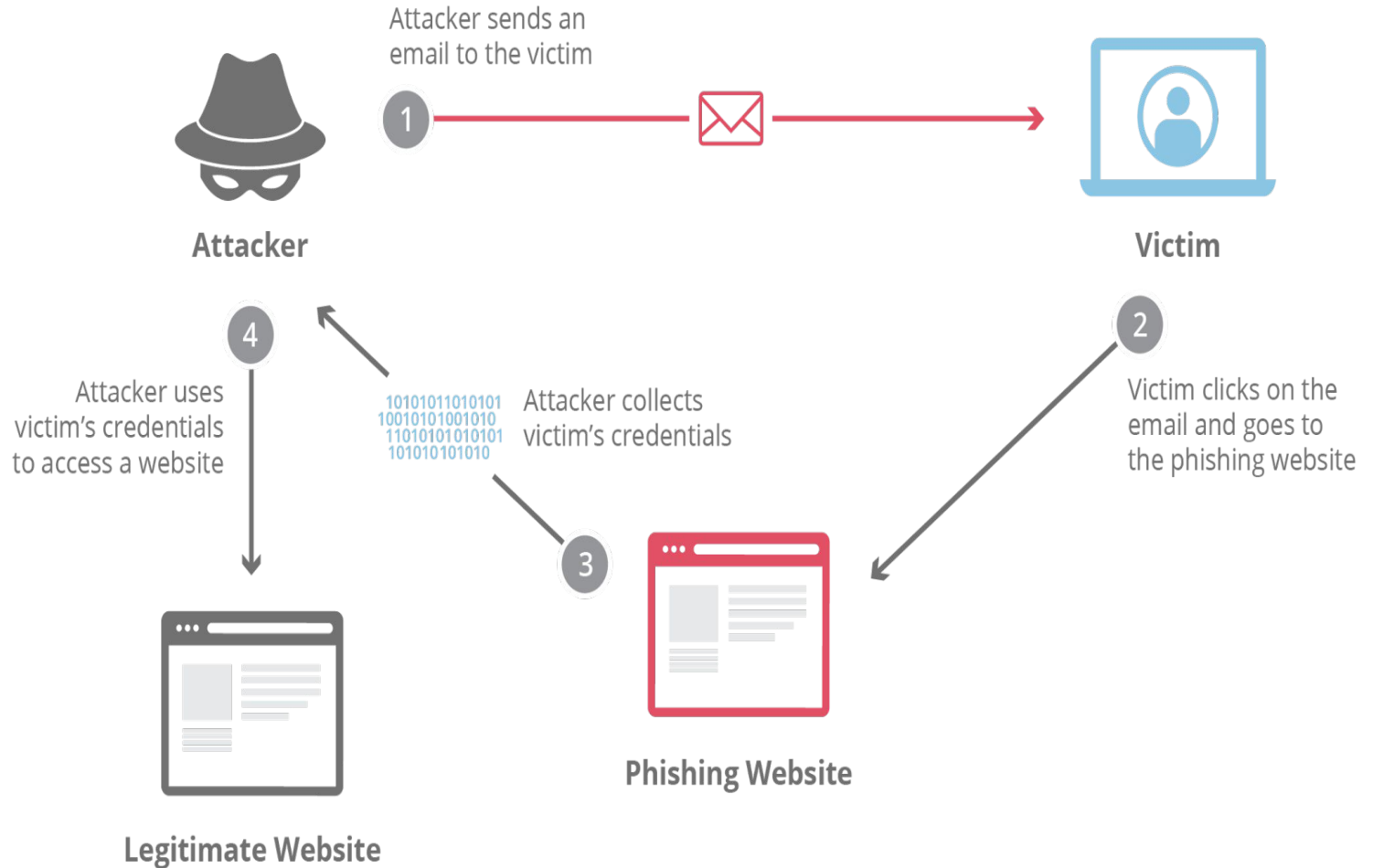
As investigações apontaram possíveis vetores de entrada que poderiam ter sido mitigados:

Vulnerabilidade em sistema legado ou ataque de *phishing*.

### **Medidas Preventivas que Deveriam Existir:**

- Programa contínuo de conscientização e treinamento contra *phishing*.
- Gerenciamento rigoroso de atualizações (*patches*) de segurança.
- Implementação de uma arquitetura de "confiança zero" (*Zero Trust*) para limitar a propagação de um ataque.

# Phishing:



## 5.5. Ações Corretivas:



- Restauração gradual dos sistemas a partir de *backups*.
- Reconstrução da infraestrutura de rede.
- Anúncio de um plano de investimento governamental para a cibersegurança em hospitais.

## 6. Caso 3 - Vazamento De Dados Do Site ATRAF (2021):



### 6.1. Descrição do Incidente:

- **Incidente:** Ataque à empresa de hospedagem Cyberserve em outubro de 2021, pelo grupo "Black Shadow".
- **Alvo:** O site de relacionamentos LGBTQ+ Atráf.
- **Ação:** Vazamento de dados altamente pessoais de cerca de 1.000 usuários, incluindo nomes, localizações e status de HIV.
- **Extorsão:** A ação foi realizada como uma maneira de extorsão digital contra a Cyberserve.
- **Desfecho:** A reputação do ATRAF e do Cyberserve foi destruída, e o site do ATRAF foi fechado.



## 6.2. Prejuízos:



### **Prejuízos Sociais e Pessoais (os mais graves):**

- Dano psicológico e social imensurável às vítimas.
- Grave violação de privacidade e exposição a estigmas.

### **Prejuízos Reputacionais e Financeiros:**

- Destruição da reputação da Cyberserve e do Atráf, inviabilizando suas operações.

## 6.3. Consequências:



### **Para as Vítimas:**

- Risco de chantagem, discriminação e *outing* (exposição da orientação sexual sem consentimento).
- Aumento da procura por suporte psicológico em linhas de emergência.

### **Para as Organizações:**

- A Cyberserve e o Atraf tiveram suas operações inviabilizadas pela perda de confiança.

## 6.4. Falhas de Segurança:



O incidente expôs falhas críticas na proteção de dados sensíveis:

### **Na Empresa de Hospedagem (Cyberserve):**

- Ausência de criptografia robusta para dados em repouso.
- Falha no monitoramento contínuo de atividades suspeitas na rede.

### **No Site (Atraf):**

- Não utilização de técnicas de anonimização ou pseudo-anonimização de dados para desassociar identidades reais de informações sensíveis, o que poderia ter limitado o dano.

## 6.5. Ações Corretivas:



- Mobilização de ONGs para oferecer suporte legal e psicológico às vítimas.
- Início de investigação pela Autoridade de Proteção de Privacidade sobre a responsabilidade da empresa de hospedagem.

## 7. Conclusão:



Através da análise individual dos casos estudados, foi possível concluir que, uma que vez que os sistemas tem se tornado cada vez mais digitais, e, visto que ataques hackers, vazamento de dados e interrupções de serviços (que tem se tornado cada vez mais frequentes) podem causar danos irreparáveis tanto financeiramente quanto socialmente aos mesmos, tem que tornado cada vez mais necessário o investimento em proteção e cibersegurança.

## 8. Referências Bibliográficas:



BLACK Shadow hackers leak data of Israeli LGBTQ dating site users. **BBC News**, 30 out. 2021.


HACKERS publish sensitive info of users on Israeli LGBTQ dating app. **The Jerusalem Post**, 30 out. 2021.

INSURANCE firm Shirbit hit by major hack, client info posted online. **The Times of Israel**, 1 dez. 2020.

ISRAELI hospital under cyber attack, patient data may be compromised. **Reuters**, 13 out. 2021.

RANSOMWARE Attack on Israeli Hospital Grinds Treatment to a Halt. **Haaretz**, 14 out. 2021.

REGULATOR finds severe deficiencies in Shirbit's information security. **Calcalistech**, 21 jun. 2021.



FORTINET. Hacking: definição, tipos, segurança e muito mais. **Fortinet**, [2025?]. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/what-is-hacking>. Acesso em: 20 out. 2025.

HACKTIVIST Cyber Attacks in the Iran-Israel Conflict. **NSFOCUS Global**, 19 abr. 2024. Disponível em: <https://nsfocusglobal.com/pt-br/the-hacktivist-cyber-attacks-in-the-iran-israel-conflict/>. Acesso em: 20 out. 2025.

LEARN Ethical Hacking Vs Malicious Hacking. **SlideShare**, 2 abr. 2024. Disponível em: <https://pt.slideshare.net/slideshow/learn-ethical-hacking-vs-malicious-hacking/267450063>. Acesso em: 20 out. 2025.

OPIsRAEL 2025: hacktivist coordination intensifies ahead of April 7. **Radware**, 28 mar. 2025. Disponível em: <https://www.radware.com/security/threat-advisories-and-attack-reports/opisrael-2025-hacktivist-coordination-intensifies-ahead-of-april-7/>. Acesso em: 20 out. 2025.

RECOVERING from a cyber incident: how can hospitals react? **Atlas Digitale Gesundheitswirtschaft**, 12 fev. 2025. Disponível em:

<https://www.atlas-digitale-gesundheitswirtschaft.de/blog/2025/02/12/recovering-from-a-cyber-incident-how-can-hospitals-react/>. Acesso em: 20 out. 2025.

SOLOMON, Shoshanna. Insurance firm Shirbit hit by major hack, client info posted online. **The Times of Israel**, 1 dez. 2020. Disponível em: <https://www.ynetnews.com/article/BkYsNqQsP>. Acesso em: 20 out. 2025.

ZIV, Amitai. Regulator finds severe deficiencies in Shirbit's information security. **Calcalistech**, 21 jun. 2021. Disponível em: <https://www.calcalistech.com/ctech/articles/0,7340,L-3879492,00.html>. Acesso em: 20 out. 2025.

O QUE é um ataque de phishing? **Cloudflare**. Disponível em: <https://www.cloudflare.com/pt-br/learning/access-management/phishing-attack/>. Acesso em: 19 out. 2025.



**Obrigado Pela Atenção!**