Principais riscos a que estão sujeitas as empresas/seguradoras

Principais Riscos Cibernéticos

1. **Ataques de Ransomware:**

Criminosos criptografam dados e exigem um pagamento para restaurar o acesso. Esse tipo de ataque está crescendo rapidamente, afetando empresas em todo o mundo.

2. **Phishing e Engenharia Social:**

Ataques que manipulam colaboradores para obter informações confidenciais ou acesso não autorizado a sistemas. O erro humano é frequentemente a porta de entrada para este tipo de ataque.

3. **Violação de Dados (Data Breach):**

Roubo ou vazamento de informações confidenciais, como dados de clientes, segredos comerciais ou informações financeiras.

4. **Negação de Serviço Distribuída (DDoS):**

Ataques que sobrecarregam os servidores de uma empresa, tornando seus serviços indisponíveis para usuários legítimos.

5. **Invasão de Sistemas:**

Hackers exploram vulnerabilidades em redes ou softwares para acessar dados ou danificar sistemas.

6. **Fraudes Cibernéticas:**

Manipulação de transações financeiras ou roubo de dinheiro via sistemas digitais, como fraudes bancárias ou invasões a carteiras digitais.

7. **Erros Internos e Falhas Operacionais:**

Inclui desde falhas humanas a erros de configuração em sistemas, que podem resultar na exposição de dados ou no comprometimento de operações críticas.

Desafios

2021: Houve um aumento de mais de **220%** nos ataques cibernéticos em comparação com o ano anterior. O país registrou aproximadamente **9,1 bilhões de tentativas de ataques cibernéticos**. *(Fonte: Fortinet)*

2022: **Mais de 30 bilhões de tentativas de ataques cibernéticos** ao longo do ano, sendo o país mais visado na América Latina, com um aumento de aproximadamente **77%** em relação ao ano anterior. *(Fonte: Kaspersky)*

2023: Até a metade de 2023, o número de ataques já ultrapassava **50 bilhões**.O Brasil foi o 3º país do mundo com o maior número de ataques de ransomware. *(Fonte: Fortinet e Check Point)*

2024: Primeiro trimestre: 38% mais ataques que no final de 2023

Segundo trimestre: aumento de 67% nos ataques, somando uma média de 2.754 ataques por organização a cada semana. *(Fonte: Check Point)*

Qual o modelo de sucesso ?

- Metodologia transparente, clara e confiável;
- Capacidade de interagir com uma organização de maneira pró-ativa, colaborativa e contínua (as vulnerabilidades e ataques não são estáticos);
- Possuir visibilidade dos riscos de empresas que podem impactor a continuidade do meu negócio;
- Poder de comunicar prioridades e planos de ação tanto para o público técnico quanto para o board da organização;
- Automatizar os processos de assessment de segurança (envio de questionários);
- Integrar soluções para maior robustez no processo de gestão de riscos de terceiros.

OBRIGADA