RANSOMWARE E EXTORSÃO DIGITAL NO AMBIENTE CORPORATIVO: EVOLUÇÃO, IMPACTOS E ESTRATÉGIAS DE DEFESA

Camilly Volk[1], Luiz Henrique Grazziotin De Oliveira[2], Vinicius Lazarotto[3], Leandro Otávio Cordova Vieira[4]

1. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
2. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
3. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
4. Docente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC

Autor correspondente: Camilly Volk, camillyvolk.k@gmail.com

Área: Ciências Exatas e Tecnológicas

Introdução: A evolução tecnológica ampliou a eficiência dos negócios, mas também a superfície de ataque das organizações, expondo-as a ameaças virtuais. Nesse cenário, o ransomware se destaca por criptografar dados críticos e exigir pagamento para liberação. Ao longo do tempo, o fenômeno evoluiu de bloqueios simples para campanhas que combinam criptografia e vazamento de informações sensíveis, configurando a dupla extorsão e elevando riscos operacionais e reputacionais. **Objetivo:** Este trabalho analisa mecanismos de operação, impactos e estratégias de defesa contra ataques de ransomware no ambiente corporativo, buscando oferecer base teórica para políticas de segurança mais robustas e adequadas à realidade digital. **Método:** A pesquisa teve duas frentes: coleta e análise de incidentes a partir de plataformas de inteligência e fontes abertas, com mineração de padrões para mapear vetores, táticas e impactos; e seleção de estudos de caso recentes com base em indicadores de comprometimento e metadados, descritos para evidenciar aspectos técnicos e dilemas éticos. Para organizar a observação, adotaram-se modelos de ciclo de ataque e catálogos de técnicas, rastreando do acesso inicial à exfiltração. **Resultados:** Os achados indicam que o ransomware, além de criptografar e paralisar sistemas, consolidou-se no modelo de dupla extorsão, em que dados sensíveis são exfiltrados e usados como pressão adicional. A cadeia típica envolve reconhecimento, entrega por vetores como phishing ou exploração de serviços expostos, instalação, movimento lateral e ação sobre o objetivo. O enquadramento por catálogos de técnicas detalha persistência, elevação de privilégios e exfiltração, evidenciando o papel de falhas de configuração e de credenciais fracas. A inteligência de ameaças sustenta a detecção ao fornecer indicadores para soluções de monitoramento, enquanto a resposta se apoia em processos de preparação, detecção e análise, contenção, erradicação, recuperação e lições aprendidas. Também se destaca a importância de cultura organizacional: treinamento contínuo, privilégio mínimo e exercícios de coordenação entre áreas técnicas, jurídicas e de comunicação, além de critérios prévios para decisões diante de exigências de resgate. **Conclusão:** Conclui-se que a mitigação eficaz requer postura proativa e defesa em profundidade: gestão rigorosa de correções, backups isolados e testados, segmentação de rede, controles de acesso com privilégio mínimo e monitoramento contínuo por ferramentas de endpoint e correlação de eventos. Somam-se capacitação contra phishing e políticas claras de resposta e comunicação. A integração entre controles tecnológicos, governança e cultura de segurança fortalece a resiliência e reduz a chance de interrupções e perdas reputacionais.

Palavras-chave: Ransomware; Dupla extorsão de dados; Cibersegurança corporativa.