ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS COM USO DE CRIPTOGRAFIA

Nylson Santos Moreira
Fatec Assis
Nylson.moreira@fatec.sp.gov.br

Fábio Eder Cardoso
Fatec Assis
Fabio.cardoso@fatec.sp.gov.br

RESUMO

Este artigo discute a importância da segurança da informação nas empresas, destacando a relevância da criptografia. Será explorada uma problemática comum enfrentada pelas empresas em relação à falta da segurança da informação, tem como objetivo a mitigação das vulnerabilidades detectadas e apresentar como as empresas podem aprimorar suas práticas de segurança para enfrentar os desafios em constante evolução.

Palavras-chave: segurança da informação, criptografia, hacker, vulnerabilidades.

ABSTRACT

This article discusses the importance of information security in companies, highlighting the relevance of encryption. A common problem faced by companies in relation to information security will be explored, the objective will be to mitigate detected vulnerabilities and it will present how companies can improve their security practices to face the constant challenges evolution.

Keywords: information security, cryptography, hacker, vulnerabilities.

1 INTRODUÇÃO

É perceptível que a tecnologia está avançando a cada dia e com isso, traz o aumento na velocidade das atividades cotidianas, como a troca de mensagens. Antigamente, as cartas poderiam demorar dias para serem entregues, enquanto hoje tem-se mensagens praticamente instantâneas. Assim as empresas precisam enviar as mensagens para as pessoas certas, no lugar certo e no tempo certo. Com tanta informação sendo compartilhada, é de suma importância que a empresa proteja esses dados contra pessoas más intencionadas.

A segurança da informação é um pilar crítico para o sucesso e a continuidade dos negócios em um mundo cada vez mais digital (Kim; Solomon, 2014). À medida que a quantidade de dados e informações confidenciais nas empresas crescem, a proteção adequada desses ativos torna-se uma preocupação premente, pois a perda dessas informações pode resultar em um grande prejuízo para a empresa. A criptografia desempenha um papel crucial na garantia da segurança da informação, fazendo com que os dados tenham uma camada de proteção a mais diante da confidencialidade, integridade, disponibilidade, dentre outros fatores, para que diminuam os riscos e ameaças sujeitos a todo o momento (Kim; Solomon, 2014). Neste artigo, apresenta os detalhes sobre a importância desses conceitos, abordando uma problemática comum, definindo um objetivo claro de melhoria e oferecendo orientações sobre como as empresas podem fortalecer suas práticas de segurança da informação.

O presente trabalho está organizado em seções: a primeira aborda as problemáticas enfrentadas pelas organizações e usuários, onde são discutidas as ameaças cibernéticas, descrevendo alguns casos de ataques a empresas. A segunda tem o objetivo de aprimorar a segurança da informação, demonstrando a importância da criptografia e auxiliando na identificação das áreas vulneráveis de uma empresa. Na terceira parte do artigo, são apresentados fundamentos e aplicações da criptografia. Por fim, nas duas últimas partes, demonstra alguns exemplos de algoritmos e aplicações e, após a identificação dos problemas, propõem-se algumas melhorias para amenizar as vulnerabilidades encontradas na segurança da informação.

Para a realização deste trabalho, será abordada uma pesquisa bibliográfica, constituída de livros, artigos e materiais disponíveis na internet por meio de fontes confiáveis. Com a intenção de interpretar, compreender e analisar as informações obtidas, serão informadas possíveis maneiras de amenizar a perda ou roubo de dados. Com isso será apresentado reflexões acerca da segurança da informação, com foco no uso de criptografia nas empresas, garantindo que os dados confidenciais estejam protegidos contra vazamentos, acessos não autorizados e corrupção. Analisando a importância da criptografia na proteção de dados confidenciais e identificando as áreas nas quais as empresas podem melhorar suas práticas de

segurança da informação e por fim demonstrar algumas recomendações práticas para a implementação eficaz da criptografia.

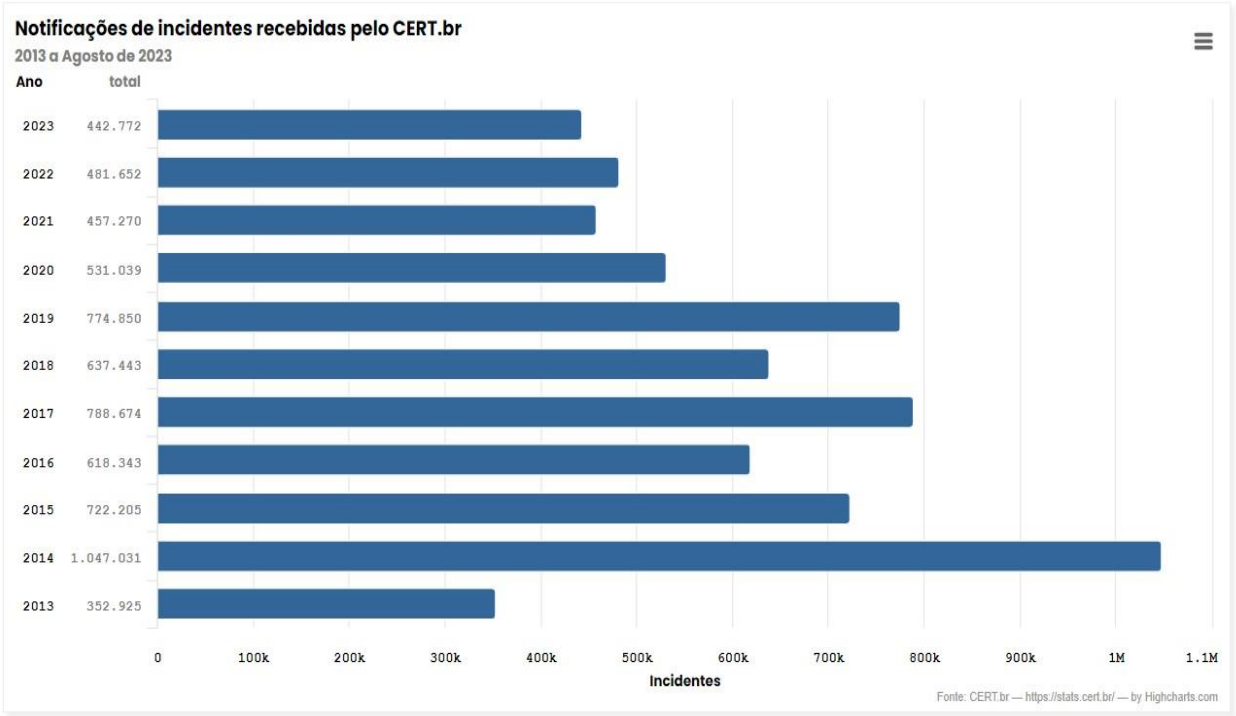
2 DESENVOLVIMENTO

2. Problemática: Desafios na Segurança da Informação

2.1. A Evolução das Ameaças Cibernéticas

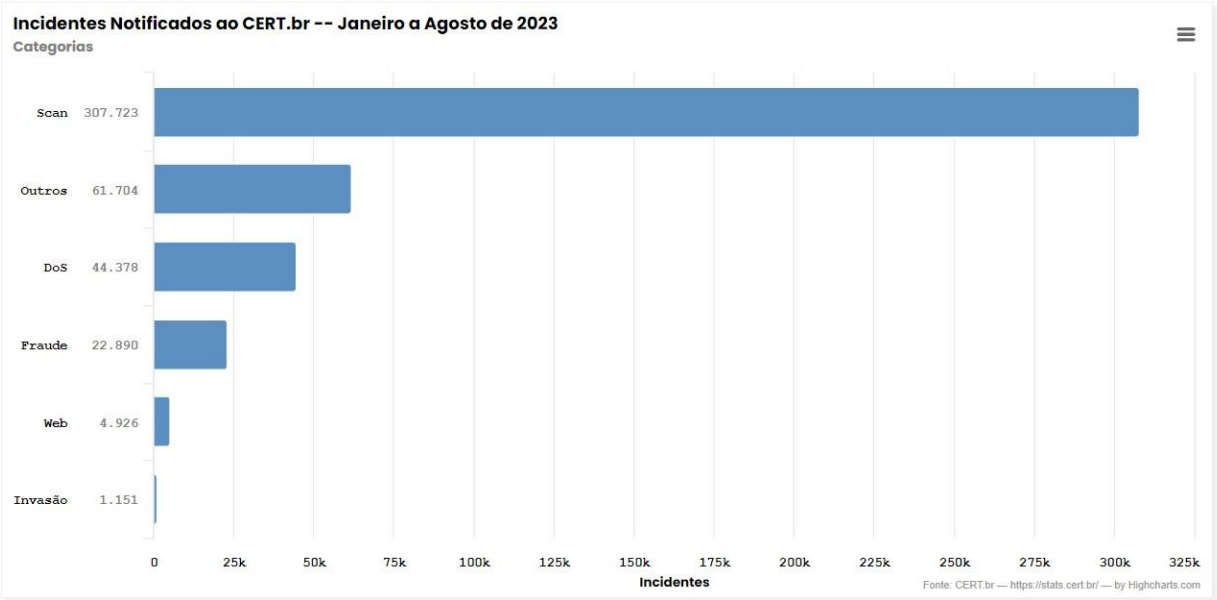
As empresas enfrentam uma ameaça constante e em constante evolução no mundo digital. Conforme a figura 1, é possível notar que nos últimos dez anos, houve uma média acima de 500 mil ataques anuais notificados ao CERT.BR. Hackers e agentes mal-intencionados estão cada vez mais sofisticados em suas táticas, visando dados valiosos e informações confidenciais. A figura 2 demonstra que muitos usuários são atacados por SCAN (engloba além de notificações de varreduras em redes de computadores, notificações envolvendo força bruta em senhas, tentativas de explorar vulnerabilidades e outros ataques sem sucesso contra serviços de rede) (CERT.BR, 2023).

Figura 1 – Notificações de incidentes recebidas pelo CERT.BR nos últimos 10 anos



Fonte: CERT.BR, 2023, Acesso em 08 nov. 2023

Figura 2 – Incidentes Notificados ao CERT.BR



Fonte: CERT.BR, 2023, Acesso em 08 nov. 2023

O problema de pesquisa detectado foi: "Como proteger os ativos de informação contra ameaças internas e externas, que estão em constante mutação?"

2.2. Dificuldade do uso de criptografia.

A adoção do uso de criptografia nas empresas pode enfrentar diversos problemas e dificuldades, sendo alguns deles:

Complexidade técnica da implementação e o gerenciamento adequado das chaves são desafios comuns. Isso pode ser agravado pela diversidade de sistemas e plataformas utilizados pelas empresas (Ferguson, 2003).

Os custos altos associados a implementação e manutenção de sistemas de criptografia, juntamente com o possível impacto no desempenho dos sistemas (Diffie, 2010).

As empresas enfrentam desafios relacionados à conformidade com regulamentações e requisitos legais específicos relacionados à criptografia em diferentes jurisdições (Solove, 2010).

2.3. Implementação da LGPD.

Com a implementação de regulamentos rigorosos, como o Regulamento Geral de Proteção de Dados (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil, as empresas enfrentam o desafio de cumprir essas normas de segurança de dados (Brasil, 2023).

No Brasil, a LGPD é um grande marco legislativo que altera o modelo de coleta e tratamento de dados pessoais, passando a coletar somente o essencial. Portanto, ela protege os

direitos e garantias da pessoa natural, tais como privacidade, autodeterminação informativa, liberdade de expressão e desenvolvimento econômico e tecnológico (Brasil, 2023).

A lei entrou em vigor em agosto de 2020, onde sua ação abrange qualquer atividade de tratamento de dado pessoal, em meio físico ou digital, desde que ocorra em território nacional. É importante destacar que a LGPD determina regras padrões de segurança da informação e medidas administrativas capazes de proteger os dados pessoais, as quais devem ser cumpridas pelos controladores e pelos operadores (Boni, 2019).

3. CRIPTOGRAFIA: FUNDAMENTOS E APLICAÇÕES

3.1. Conceitos Básicos de Criptografia

No contexto de criptografia, podem se destacar dois métodos, sendo eles: a simétrica, onde o ciframento da mensagem é baseado no algoritmo e na chave de segurança; os dois trabalham juntos, de forma que tornam o conteúdo protegido com um conjunto único de regras. Sendo assim, a criptografia simétrica utiliza apenas uma chave, que é compartilhada entre o emissor e o destinatário. Sua vantagem é a boa performance e uma comunicação contínua simultaneamente entre várias pessoas. Porém, são necessárias duas chaves para cada pessoa na comunicação, e não há um ambiente seguro para armazenar as chaves de segurança (Oliveira, 2012).

Dentre os algoritmos de criptografia simétrica, o AES (*Advanced Encryption Standard*) é um dos mais utilizados. Ele foi desenvolvido pelo NIST (*National Institute of Standards and Technology*) e possui três variações, com tamanhos de chaves de 128, 192 e 256 bits (Singh, 2011).

A criptografia assimétrica é baseada em chave pública e privada, sendo usadas para cifrar a mensagem e verificar a identidade do usuário. Tem como vantagem garantir a privacidade do usuário e a confiabilidade na troca de dados (Kim; Solomon, 2014).

Dentre os algoritmos de criptografia assimétrica, o RSA (Rivest-Shamir-Adleman) é um dos mais conhecidos. Ele é baseado na teoria dos números e na fatoração de números primos grandes. O RSA é utilizado em assinaturas digitais e chave de sessão (Oliveira; Cruz; Gomes, 2018).

Contudo, o uso de criptografia é necessário para a proteção das informações armazenadas ou trocadas entre os usuários. Pode-se analisar e escolher entre os dois tipos descritos, qual melhor se encaixa na situação.

3.2. Aplicações da Criptografia nas Empresas

As empresas possuem diversas informações armazenadas, sendo necessário alguns métodos de segurança, onde os ataques geralmente são na tentativa de obter acesso ou comprometer esses dados. Alguns dos métodos para amenizar são o controle de acesso, o isolamento de alguns dados e evitar conceder acesso público (Silva, 2012).

Em qualquer organização, é importante manter uma comunicação segura durante a troca de informações, evitando que vaze qualquer dado e minimize os possíveis efeitos e perdas, onde é necessário garantir a confidencialidade e a autenticidade dos dados.

Conforme a quantidade de funcionários na empresa, é interessante delimitar o acesso de cada um, onde nem todos precisam ter acesso às informações mais importantes. Com isso, seria ideal salvar as credenciais em locais seguros e utilizar mais de um método de acesso, como, por exemplo, a biometria (Silva, 2012).

Por fim, as empresas precisam estar em dia com a conformidade regulatória, para garantir uma maior segurança a respeito de softwares maliciosos ou piratas, podendo facilitar a detecção e prevenção de ataques (Rezende, 2005).

4 APRIMORANDO A SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

4.1. Avaliação de Riscos

Cada área da empresa precisa funcionar conforme foi estabelecido, porém é preciso identificar as mais importantes (o coração da empresa) para protegê-las a todo custo. Os ativos importantes dentro de uma corporação podem ser uma pessoa, uma informação, uma senha, uma máquina, todos podendo sofrer ameaças ambientais ou humanas (Inteco, 2010).

Dentre as vulnerabilidades, uma das mais comuns ocorrem nos meios físicos utilizados para guardar informações de extrema importância, que podem ser danificados ou acessados de diversas maneiras, até mesmo por pessoas indevidas dentro da companhia (Macêdo, 2014).

Por outro lado, as pessoas que têm acesso a tais informações precisam tomar cuidado ao falar em celulares, corredores ou locais públicos. É de extrema importância priorizar as medidas de segurança necessárias, por mais simples que pareçam ser. Qualquer descuido pode ser suficiente para que alguma pessoa maliciosa invada ou acesse tais informações (Sêmola, 2003).

Por fim, o mapeamento dos ativos críticos deve ser realizado de acordo com a importância de cada informação ou setor para a empresa, determinando normas e procedimentos para acessá-las, o nível de segurança e o controle de acesso.

4.2. Políticas de Criptografia

É imperativo que as empresas determinem algumas políticas de segurança para evitar perda ou vazamento de dados. Esse controle envolve desde regras até programas de proteção, sendo um planejamento necessário para aumentar a confidencialidade, integridade e disponibilidade das informações. Após isso, é necessário determinar quais dados e os tipos de proteções utilizados, por exemplo: separando as informações por grau de importância para a corporação, podendo implementar o que cada usuário poderá acessar com suas respectivas senhas de login (Sêmola, 2003).

4.3. Treinamento e Conscientização

Educação e treinamento dos funcionários sobre práticas de segurança são fundamentais para uma maior proteção, onde os funcionários devem saber o que estão acessando e o que podem fazer para deixar um ambiente mais seguro.

Com um treinamento adequado os funcionários têm um conhecimento maior sobre criptografia, o que ameniza a possibilidade de ataque e diminui as vulnerabilidades (Inteco, 2010).

A implementação de sistemas de monitoramento para detecção de atividades suspeitas, podendo rodar algum *software* com determinada frequência, visa um maior controle de segurança. As empresas podem efetuar uma auditoria regular das práticas de segurança da informação.

É possível notar que *hackers* e *crackers* estão sempre inovando, aparecendo com novos métodos de acesso e roubo de informações. Devido a isso, é importante o acompanhamento das evoluções tecnológicas e regulatórias, atualizando os sistemas de segurança e os treinamentos. Observar e se adaptar às novas ameaças é de grande importância para a organização (Inteco, 2010).

5 CONSIDERAÇÕES FINAIS

Diante da análise sobre a segurança da informação nas empresas, com foco nas práticas de criptografia, torna-se evidente a complexidade do cenário atual, marcado pela constante evolução tecnológica e pelas ameaças cibernéticas cada vez mais sofisticadas. Este contexto destaca a necessidade premente de estratégias robustas de proteção de dados, especialmente diante do cenário em que as organizações se encontram.

A proteção dos ativos de informação é de grande importância, considerando não apenas os desafios enfrentados pelas organizações, mas também as regulamentações que regem o tratamento de dados pessoais. No contexto brasileiro, a Lei Geral de Proteção de Dados (LGPD) estabelece padrões rigorosos para as práticas relacionadas ao manejo de informações pessoais, tornando imperativa a conformidade das empresas a fim de evitar penalidades e garantir a privacidade dos indivíduos.

Para fortalecer a segurança da informação, as empresas devem adotar uma abordagem holística. Isso inclui não apenas a implementação de tecnologia avançada, como criptografia, mas também a realização de avaliações contínuas de riscos. O estabelecimento de políticas claras relacionadas à proteção de dados e o investimento significativo em treinamento e conscientização dos funcionários são elementos cruciais nesse processo.

A adaptação constante às mudanças tecnológicas e regulatórias é uma exigência para garantir uma postura defensiva eficaz diante das ameaças emergentes. Isso envolve não apenas a atualização de sistemas de segurança, mas também a revisão contínua das práticas adotadas, a fim de incorporar as melhores estratégias diante do dinamismo do ambiente digital.

Em suma, a segurança da informação nas empresas transcende a mera adoção de tecnologias pontuais. É uma abordagem abrangente que requer entendimento, planejamento e constante atualização para garantir a proteção efetiva dos dados em um ambiente corporativo cada vez mais desafiador.

6 REFERÊNCIAS

BONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Lei/L13709.htm.

Dang, Q. H. (2015). **Secure hash standard. Technical report**, NIST

DIFFIE, Whitfield; LANDAU, Susan. **Privacy on the line: The politics of wiretapping and encryption**. The MIT Press, 2010.

FERGUSON, Niels; SCHNEIER, Bruce. **Practical cryptography**. New York: Wiley, 2003

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

INTECO, National Institute for Communications Technologies. **Taxonomy information security taxonomy hand-book**. León, Espanha: Gráfica Alse. Fevereiro de 2010.

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação**.
Rio de Janeiro: LTC, 2014. 385 p. ISBN 978-0-7637-9025-7.

MACÊDO, Diego. **Modelos e mecanismos de segurança da informação**, 2014. Disponível em: <https://www.diegomacedo.com.br/modelos-e-mecanismos-de-seguranca-da-informacao/>

OLIVEIRA, I. D. H. F.; CRUZ, M. P. M. D.; GOMES, R. L. R. **A relação científica entre a criptografia e os números primos**. Revista Atlante: Cuadernos de Educación y Desarrollo, n. 1-20, p. 20, 2018.

OLIVEIRA, R. R. **Criptografia simétrica e assimétrica-os principais algoritmos de cifragem.** Segurança Digital [Revista online], v. 31, p. 11–15, 2012.

OLIVEIRA, Wilson José de. **Segurança da Informação: Técnicas e Soluções**. Florianópolis: Visual Books Ltda, 2001.

REZENDE, Denis Alcides. **Engenharia de Software e Sistemas de Informação**. 3ª ed. Rio de Janeiro: Brasport, 2005

SÊMOLA, Marcos. **Gestão da Segurança da Informação, uma visão Executiva**. Rio de Janeiro: Elsevier, 2003.

SILVA, Antônio Everardo Nunes da. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2012.

SINGH, S. **O livro dos códigos**. 9º edição. ed. Rio de Janeiro: Record, 2011. 446 p. ISBN 8501055980.

SOLOVE, Daniel J. **Understanding privacy**. Harvard university press, 2010.