PROJECT, DESIGN AND MANAGEMENT

ISSN: 2683-1597

PROJECT DESIGN & MANAGEMENT

Cómo citar este artículo:

Quissanga, F. C. & Fernandes, R. F. (2020). Importância da segurança da informação nas empresas corporativas do ramo da tecnologia de informação. *Project, Design and Management, 2*(1), 87-102. doi: 10.35992/pdm.v2i1.431

IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS CORPORATIVAS DO RAMO DA TECNOLOGIA DE INFORMAÇÃO

Fernando Cassinda Quissanga
Universidad Internacional Iberoamericana (México), Universidad Europea del Atlántico (España)
fernandoquissanga@hotmail.com · https://orcid.org/0000-0003-4468-7206
Roberto Fabiano Fernandes
FUNIBER – Fundación Universitaria Iberoamericana / Faculdade Cesusc / Universidade do sul de Santa Catarina (Brasil)
roberto.fabiano@unini.org · https://orcid.org/0000-0002-6738-6572

Resumo. A importância da segurança da informação nas empresas corporativas no ramo da tecnologia da informação tem como o objetivo primário em propor medidas de segurança para proteger a informação nas empresas corporativas do ramo da tecnologia de informação. Neste sentido, a pesquisa é qualitativa, de cunho exploratório e descritivo, pois tem como base a busca por material bibliográfico que possibilite sugerir medidas de segurança para a proteção das informações. Os dados secundários foram coletados de forma sistemática, buscando-se pela palavra chave – medidas de segurança e seus sinónimos. Realizou-se a busca em bases de dados computadorizadas, como o Google Académico® e o Portal de Periódicos Capes. Identificou-se um conjunto de sugestões de medidas de segurança que possibilitem as empresas corporativas do ramo da Tecnologia da Informação possam usufruir. Destaca-se como conclusão que as medidas preventivas, detetivas e corretivas propostas devem estar envolvidas em um plano de segurança e contingência disseminadas em toda a organização.

Palavras-chave: Segurança da informação, Medidas de Segurança, Empresas corporativas.

IMPORTANCE OF INFORMATION SECURITY IN CORPORATE INFORMATION TECHNOLOGY COMPANIES

Abstract. The importance of information security in corporate information technology companies has the primary objective of proposing security measures to protect information in corporate information

technology companies. In this sense, the research is a qualitative, exploratory and descriptive, as it is based on the search for bibliographic material that makes it possible to suggest security measures for the protection of information. Secondary data were collected systematically, looking for the keyword - security measures and their synonyms. The search was carried out in computerized databases, such as Google Académico® and the Portal de Periódicos Capes. A set of suggestions for security measures that enable corporate companies in the field of Information Technology to take advantage of has been identified. It is highlighted as a conclusion that the proposed preventive, detective and corrective measures must be involved in a security and contingency plan disseminated throughout the organization.

Keywords: Information security, Security measures, Corporate companies.

IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE TECNOLOGÍA DE INFORMACIÓN CORPORATIVA

Resumen. La importancia de la seguridad de la información en las empresas corporativas de tecnología de la información tiene el objetivo principal de proponer medidas de seguridad para proteger la información en las empresas corporativas de tecnología de la información. En este sentido, la investigación es cualitativa, exploratoria y descriptiva, ya que se basa en la búsqueda de material bibliográfico que permita sugerir medidas de seguridad para la protección de la información. Los datos secundarios se recopilar on sistemáticamente, buscando la palabra clave: medidas de seguridad y sus sinónimos. La búsqueda se realizo en bases de datos computarizadas, como Google Académico® y el Portal de Periódicos Capes. Se ha identificado un conjunto de sugerencias para medidas de seguridad que permiten a las empresas corporativas en el campo de la tecnología de la información aprovechar. Se destaca como conclusión que las medidas preventivas, de detección y correctivas propuestas deben estar involucradas en un plan de seguridad y contingencia difundido en toda la organización.

Palabras clave: Seguridad de la información, Medidas de seguridad, Empresas corporativas.

Introdução

A segurança da informação tem sido uma preocupação em todo mundo, a informação tornou-se muito importante, e o seu manuseio requer muitos cuidados, sendo necessário criar condições para proteger. Desta forma, é impossível dizer que estamos totalmente seguros, mesmo quando se trata da segurança de países do primeiro mundo. Isso se deve porque as perdas económicas, problemas psicológicos, deontológicos e ideológicos são muito avultados, no século presente nos deparamos com várias dificuldades para controlar o cibercrime (*Brute force*) e espionagem (*Sniffing*).

Entende-se *Sniffing*, segundo a definição do site CERT.br (2012 p.19), *"Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers."*

No entanto os golpes de estados, as fraudes eleitorais, vazamento de informação política, segredos de estado e desvios bancários (que denominam-se a técnica de *phishing*) têm sido uma preocupação. O roubo por cartões de créditos como a clonagem de cartões de créditos, falsificação de *e-mail* (*E-mail spoofing*), alteração de notas na base de dados das universidades (*Pharming*).

Entretanto é oportuno falar que a segurança da informação tornou-se a primeira inquietação que relata-se neste artigo. Em 2018 a maior preocupação dos países foi a de criar legislação para evitar o crime e poder levar a justiça os prevaricadores, porque é muito difícil detetar quando estamos a ser alvos de um crime informático. Mecanismos básicos de segurança devem ser estudados de forma profunda, como a identificação, autenticação, autorização, integridade, confidencialidade e disponibilidade da informação.

Neste mesmo caminho, entende-se que o advento das redes sociais também permitiram aumentar o número de ataques de vírus informáticos, espiões para cópias de credenciais, senha de utilizadores, códigos diversos a enviar para um computador remoto onde os *Crackers* buscam essas informações para cometer crimes. Outra técnica muito usada pelos *Crackers* é a engenharia social, a qual tem como objetivo de ludibriar pessoas no intuito de ter o acesso a informações que permitam invadir computadores ou dispositivos computacionais.

Com base nestas descrições, tem-se como objetivo geral deste artigo sugerir medidas de segurança para proteger a informação nas empresas corporativas do ramo da tecnologia de informação.

Método

Entende-se esta pesquisa como qualitativa, de cunho exploratório e descritivo, pois tem como base a busca por material bibliográfico que possibilite sugerir medidas de segurança para a proteção das informações. Os dados secundários foram coletados de forma sistemática, buscando-se pela palavra chave – *medidas de segurança* e seus sinónimos. Realizou-se a busca em bases de dados computadorizadas, como o Google Académico® e o Portal de Periódicos Capes. O Google Académico® para Creswell (2010) é uma base de dados gratuita que proporciona amplitude na busca na literatura de várias fontes, como teses, resumos e artigos, com a vantagem de poder obtê-los de forma integral. Quanto ao portal de Periódicos da Capes, ele foi escolhido como fonte de busca por oferecer acesso aos textos completos de artigos selecionados em mais de 15.000 revistas internacionais, nacionais e estrangeiras, e 126 bases de dados com resumos de documentos em todas as áreas do conhecimento (Portal de periódicos capes). Quanto a análise, considera-se o uso da análise descritiva dos dados, pois a mesma permite organizar, resumir e descrever os aspetos importantes de um conjunto de características observadas ou comparar tais características entre dois ou mais conjuntos.

Descrição das principais perdas económicas provocadas pela falha da segurança da informação

Com base na busca literária, identificou-se algumas perdas económicas quando não se tem precaução e controle ou o uso e aplicação de medidas baseadas na segurança da informação.

Entretanto Coopamootoo (2018) sugeri as empresas a proteção da privacidade dos funcionários em interações *on-line*:

> Em interações *off-line*, precisamos divulgar informações sobre nós mesmos para criar confiança com outras pessoas. Quando nos movemos *on-line*, existem diferenças: as empresas precisam estar envolvidas para facilitar a interação *on-line* e precisam manter informações sobre nós para fazer isso.

> Essas empresas têm o dever de proteger a nossa privacidade, mas nossa informação pode estar em risco de perda acidental de dados ou ataques maliciosos.

No entanto, a proteção e privacidade das informações tem sido uma preocupação e receio dos usuários que possuem serviços nessas empresas. A vulnerabilidade dos dados que podem ser utilizados para ataques cibernéticos, não só para roubos informáticos no caso de dados bancários, mas também pelo emprego da engenharia social e assim como nas redes sociais.

A maior parte dos utilizadores da tecnologia moderna de informação correm muitos riscos, pois permitem falhas pela falta de precaução e domínio de causa. Muitos não possuem preparação específica sobre segurança da informação, sendo que, a preparação tem que estar na base dos conhecimentos, todos devemos conhecer essas técnicas de segurança da informação para que aja proteção, porque a experiência mostra que, não só os usuários, mas também as empresas permitem maior parte das vezes expor os dados dos seus clientes como cita-se a Futurelearn (2018):

> O ataque cibernético da *Talk Talk* viu os detalhes pessoais de 157.000 clientes, incluindo detalhes do cartão de crédito, sendo divulgados em outubro de 2015. Como resultado, a empresa perdeu cerca de £ 60 milhões e mais de 100.000 clientes, mas os clientes também estavam abertos a potenciais fraudes de identidade: em alguns casos, os fraudadores usaram os dados para permitir que eles possuíssem como engenheiros da *Talk Talk*, contatando clientes e persuadindo-os a instalar *malwares* em suas máquinas.

No entanto, deparamos com uma situação precária, notamos que para além da empresa falhar com o sistema de segurança, os clientes também facilitam o furto de dados, por não possuírem conhecimentos de segurança da informação e permitem os criminosos implementarem a engenharia social.

Entretanto, os ataques cibernéticos nos últimos anos têm trazido muitas dificuldades, os *malwares* pertencentes a vários grupos dos vírus informáticos aproximadamente de 31 famílias presentes, exemplo o *trajon*, *worms* ou vermes, *dropper* e *backdoor*, estão na base de muitas perdas económicas, a falsa identidade, a espionagem, o roubo de dados, os tipos de fraudes informáticos e o envio de dados para um computador remoto, mesmo que estejam geograficamente distantes ou em continentes diferentes.

Os investimentos na área financeira correm riscos severos, os atacantes estão na base destas situações evoluindo o cibercrime e ciberterrorismo, os clientes são os seus alvos, porque muitas vezes têm negligenciado e permitem que seus dados sejam furtados, sendo que através dos furtos digitais dos clientes a empresa é afetada da mesma forma o seu sistema de segurança, também por vezes a empresa permite o roubo de informações, quando não possui um sistema de segurança adequado para proteção dos seus dados.

No entanto, a empresa e os clientes devem estar protegidos para impedir que pessoas não autorizadas têm acesso as suas credenciais e estejam munidos de todas ferramentas de segurança da informação, pelo que as empresas corporativas e não só, devem estar preparadas para evitar perdas económicas ocasionados pela falha da segurança dos clientes, usuários, funcionários, e antigos trabalhadores, que já conhecem todo sistema de segurança. Neste caso é importante revitalizar e reestruturar todo sistema de segurança para evitar situações do género, as políticas de segurança não devem ser conhecidas por terceiros, isso torna vulnerável a empresa.

Ainda falando sobre fraudes em cartões de créditos no Reino Unido é oportuno apresentar o gráfico das perdas económicas das fraudes ao longo dos anos:

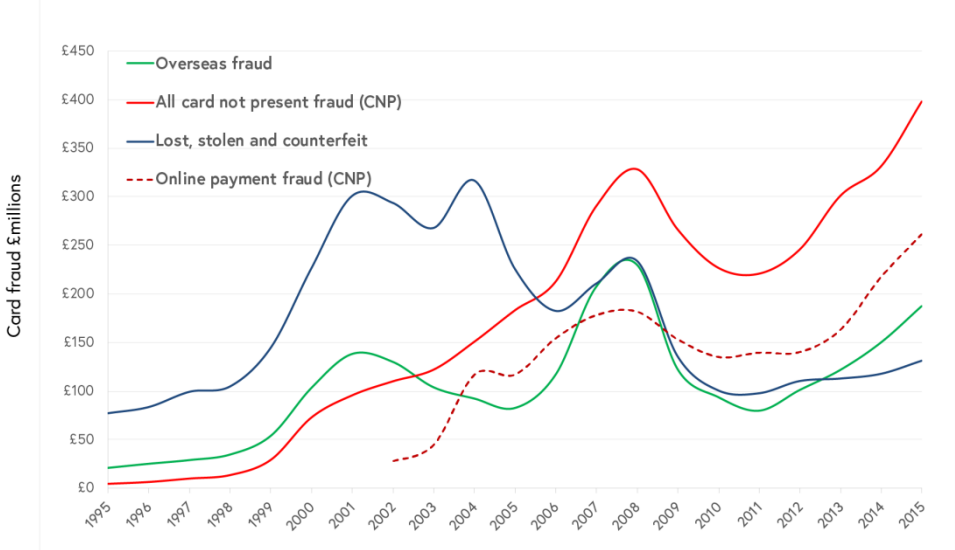

Figura1. Gráfico de perdas anuais com cartões emitidos no Reino Unido
*Nota:*Fonte: Futurelearn (2018).

É possível observar na figura 1, que desde o ano de 1995 à 2015 houve um aumento substancial de ataques informáticos nos cartões de créditos, que resultou de perdas financeiras na escala de 0 euros a 450 milhões de euros, valores estes que as empresas estão sujeitas a falir. As empresas corporativas que o seu capital financeiro é maior estão sujeitas a perderem mais quando não se tem prevenção contra os *Crackers* e as pragas virtuais.

Na figura 1, pode-se verificar que os pagamentos fraudulentos feitos *on-line* apresentam uma escala acima de 250 milhões de euros, muito dinheiro roubado por fraude financeiro, por isso, é necessário prevenirmo-nos para impedir os crimes virtuais.

No caso de roubos, perdas e falsificação citados na figura 1, menciona-se uma escala acima dos 300 milhões de euros.

No entanto, a figura 1, faz referência também à cartões de créditos efetuados sem fraude bancários, na ordem dos 400 milhões de euros.

Segundo Ação de Fraude Financeira no Reino Unido (2017, p. 10): apresenta as perdas económicas feitas por roubos através de pagamentos *on-line* com cartões de créditos: "*Perdas de fraude financeira em cartões de pagamento, bancos remotos e cheques totalizaram £ 768,8 milhões em 2016, um aumento de 2% em relação a 2015."* Entretanto, são inúmeras dificuldades e perdas económicas por falta de segurança da informação, notamos muitas vezes, algumas empresas exporem os nossos dados e isso tem causado geralmente a fraude, e muitos procuram da empresa uma indemnização, outros nem por isso, se tornam calados sem saber onde recorrer, neste caso, temos que ter muito cuidado, como e onde colocamos as nossas credenciais, o tipo de redes sociais em que pertencemos, o tipo de negócio ou compra *on-line*, todos esses fatores devem ser tratados com especial atenção.

> Novas tecnologias erradicam as formas existentes de cometer fraudes, mas também introduzem outras vulnerabilidades que os fraudadores adaptam para

> aproveitar. Chip e PIN dificultavam o uso de um cartão roubado e, portanto, o roubo de cartões declinava. No entanto, os criminosos identificaram que o pagamento *on-line* se tornou um ponto fraco, uma vez que não pode usar *Chip* e *PIN*. A fraude *on-line* é agora a forma mais comum de fraude de pagamento no Reino Unido (Ação de Fraude Financeira no Reino Unido, 2017, p. 18).

Diante desta fraude, o que destaca-se é que todo profissional do banco deve estar preparado para saber gerir a gestão documental e de processos, e por sua vez a informação e o património financeiro, deve comportar-se como um profissional que tem o banco como sua bandeira, não sabemos de concreto o que esteve na base de extorquir, mas pensamos que os bancos devem promover um salário equilibrado para o seu pessoal técnico, como formação nos domínios da segurança da informação, ética e deontologia profissional.

Segundo o Site Terra (2018):

> O vazamento de 11,5 milhões de documentos – os chamados de *Panama Papers* – do escritório panamenho de advocacia e consultoria Mossack Fonseca, a quarta maior empresa de advocacia *offshore* do mundo, teria revelado detalhes de centenas de milhares de clientes que utilizam paraísos fiscais no exterior supostamente para evasão fiscal, lavagem de dinheiro, tráfico de drogas e armas.

Além da análise de Bancos, faz-se também uma abordagem sobre as duas empresas corporativas de telefonia móvel celular, que podemos designar como concorrentes a Samsung e a *Apple*. Essas empresas possuem um sistema de segurança muito robusto, têm muitos especialistas em segurança da informação, para proteger os protótipos, as patentes e a indústria telefónica. No entanto estas empresas são líderes no mercado internacional de telefonia, mas se não forem empregues métodos avançados de segurança da informação nessas empresas uma falha é fatal, todo cuidado é pouco, neste caso temos que estar precavidos para evitar situações desastrosas, como em 2012 na Califórnia a Samsung acusada de ter violado patentes somente para aparência dos aparelhos e a funções *touch*, que foi obrigada a indemnização de milhões de dólares, imaginamos que seja um protótipo, o escândalo seria maior. Neste acontecimento a empresa sul-coreana foi forçada a indemnizar, segundo a Oficina Net, (2015):

> Em 24 de agosto de 2012, um júri de San José, na Califórnia, declarou a *Samsung* culpada pela violação de uma série de patentes de sua maior concorrente, o mesmo júri sentenciou a empresa sul-coreana a pagar o equivalente a US$ 930 milhões de indemnização à *Apple*. Por sua vez, a corte de apelação federal de *Washington*, nos Estados Unidos, confirmou, em partes, a decisão do júri de San José, tentando reverter parte da sentença, alegando que a Samsung foi condenada injustamente por violar as patentes vinculadas somente à aparência dos aparelhos e às funções "*touch*" do dispositivo móvel da empresa *Apple*.

Algumas práticas na insegurança da informação

Depois dos danos ocasionados pelas principais perdas económicas provocadas pela falha da segurança da informação é oportuno mencionar diversas práticas que permitem falhas da segurança da informação. A maior parte dos utilizadores da informação possibilitam que essas falhas aconteçam, porque um número maior deles apresentam uma educação inadequada para a proteção de dados informáticos, que

possibilita, ou seja, se traduz em uma porta aberta para os criminosos virtuais, os *Crackers* e espiões informáticos que aproveitam para cometer os crimes cibernéticos.

De acordo com Laureano (2005, p. 15 apud Shirey, 2000) temos a definição de alguns termos importantes no tocante à segurança da informação:

> Ameaças
>
> Em inglês, utilizamos o termo "*threat*" para definir ameaça. E temos vários tipos de *threat*:
>
> - Ameaça Inteligente: Circunstância onde um adversário tem a potencialidade técnica e operacional para detetar e explorar uma vulnerabilidade de um sistema;
> - Ameaça: Potencial violação de segurança. Existe quando houver uma circunstância, potencialidade, ação ou evento que poderia romper a segurança e causar o dano;
> - Ameaça de Análise: Uma análise da probabilidade das ocorrências e das consequências de ações prejudiciais a um sistema;
> - Consequências de uma ameaça: Uma violação de segurança resultado da ação de uma ameaça. Inclui: divulgação, usurpação, deceção e rompimento.

As ameaças são várias como podemos observar que os fraudadores utilizam muito a engenharia social fazendo-se de autênticos de um determinado banco ou serviço, persuadindo o cliente a cadastrar-se, para poder roubar as suas credenciais, a internet sobre tudo as redes sociais permitem o acesso indevido da informação, fazendo menção uma das vias mais velozes de propagação de vírus informáticos são os *sites* pornográficos. Os criminosos têm sido dos seus preferidos porque até alguns, adolescentes, e adultos desconhecem que os criminosos utilizam esses *sites* para roubos informáticos. Sendo que a contaminação acontece quando fazermos a abertura da imagem ou vídeo, neste caso, os vírus têm a capacidade de apresentar-se como anexo ao documento, e replicam-se ao hospedeiro num curto espaço de tempo.

Segundo Martinelli (2008, p. 46):

> Muitos vírus se disfarçam como supostos jogos, funcionalidades, em arquivos anexos. Criadores de vírus também usam engenharia social para alcançarem as suas vítimas, alegando cadastros a instituições governamentais, segurança, pornografia e diversão gratuita. Mensagens de textos infetadas às vezes substituem a linha do remetente se passando por pessoas conhecidas, aumentando as chances de contaminação.

Entretanto, os vírus informáticos são tão ágeis e destrutivos no processo de transmissão, que cada um apresenta a sua especificidade. Porém, a regra é a mesma e baseia-se no comportamento dos vírus biológicos ao ataque nas células humanas, já os vírus informáticos atacam os sistemas operacionais nos seus respetivos arquivos. Toda empresa que lida com a informação deveria possuir uma sala de controle da segurança da informação para impedir que seus dados sejam perdidos. Há nessa recomendação o dispêndio de todo investimento na segurança da informação, sendo importante contratar especialistas na área de segurança da informação ou criar um departamento que vela pela arquivologia e gestão documental. As empresas queixam-se de vários furtos informáticos porque um número considerado delas não investem na proteção dos dados.

As empresas corporativas devem dar exemplo na proteção dos dados, não devem desperdiçar a informação porque estão sujeitas a perder reputação e outras perdas financeiras. Por exemplo, pode-se mencionar a empresa Coca-Cola, quem não gostaria de saber a fórmula do seu refrigerante.

Entretanto, grandes empresas nunca fracassaram e sempre diferenciaram-se por protegerem o seu património. Procurem imaginar o sistema de segurança que essas empresas possuem, que obriga muito controle e investimento. No entanto, entende-se que essa cultura deveria ser transportada para outras empresas corporativas.

De acordo com Laureano (2005, p. 17):

> Para implementar mecanismos de segurança faz-se necessário classificar as formas possíveis de ataques em sistemas:
>
> - Intercetação: considera-se intercetação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).
> - Interrupção: pode ser definida como a interrupção do fluxo normal das mensagens ao destino.
> - Modificação: consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.
> - Personificação: considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade.

Ao abordar sobre o mecanismo de segurança da informação é necessário fazer menção ao tipo de segurança física (*Hardware*) e lógica (*Software*). Elas devem ser estudadas de forma profunda porque, na maioria das vezes, nos precavemos mais em uma e não em outra. Orienta-se que não adianta possuir um mecanismo de segurança lógico (*Software*) robusto e um sistema de segurança física (*Hardware*) desprotegido, o que pode acontecer é o roubo dos dispositivos informáticos.

Sugere-se que devemos estar preparados para as duas formas de segurança da informação e deve-se investir bastante para a que haja proteção nas nossas instalações e num dado perímetro.

Traçar as diferentes formas de roubos informáticos

Para Oliveira (2009, p. 14-15) as ameaças organizacionais são divididas em cinco:

- Ameaças físicas;
- Ameaças lógicas;
- Ameaça ocupacional;
- Ameaça à confidencialidade;
- Ameaça ambiental.

Apesar de ocorrerem várias ameaças nas empresas, neste momento daremos ênfase as ameaças físicas e as lógicas, por ser alvo da nossa pesquisa.

> Entretanto, *malware* são *softwares* feitos com objetivo infetar qualquer programa. Os *worms* têm a capacidade de se replicar. Os *spywares* são programas feitos para espiar os usuários e recolhe informações para monitorar a vítima. O *phishing* é enviado geralmente por correio eletrónico e captura informações extremamente confidenciais para posteriormente efetuar a fraude (Quissanga, 2015, p. 6).

Entretanto é sabido que existe vários tipos de crimes informáticos, os efetuados por meio de computadores, executados por meio de internet, de forma tecnológica, de forma digital, e outros crimes de índole jurídico. O roubo informático é mais abrangente, pelo que, alguns não possuem uma legislação, regulamento ou código penal, ainda no contexto atual países veem estudando métodos para prenderem os criminosos virtuais, tarefa que não tem sido fácil, alguns são julgados muito distantes da realidade, assim como artigos ou decretos empregues fora do contexto prejudicando ou beneficiando os prevaricadores, no entanto, o controle dos roubos informáticos deve ser feito um estudo mais profundo e aturado, implementar medidas detetivas, porque existem várias formas de ataques cibernéticos.

No entanto, as empresas têm que estar preparadas para impedir os ataques, isso passa por utilizar todos dispositivos de segurança tanto a lógica e física e formar o seu pessoal técnico ou contratar empresas especializada na área de segurança da informação, no caso de não possuir todas ferramentas de segurança. Quando estamos expostos na internet, mais vulneráveis nos tornamos, por esse motivo precisamos implementar o *firewall* para impedir tráfegos desnecessários que podem ser uma via de transmissão de vírus informáticos, neste caso todos pacotes estranhos, ou seja, não autorizado o *firewall* elimina, denega todos pacotes suspeitos, só permitindo os autorizados.

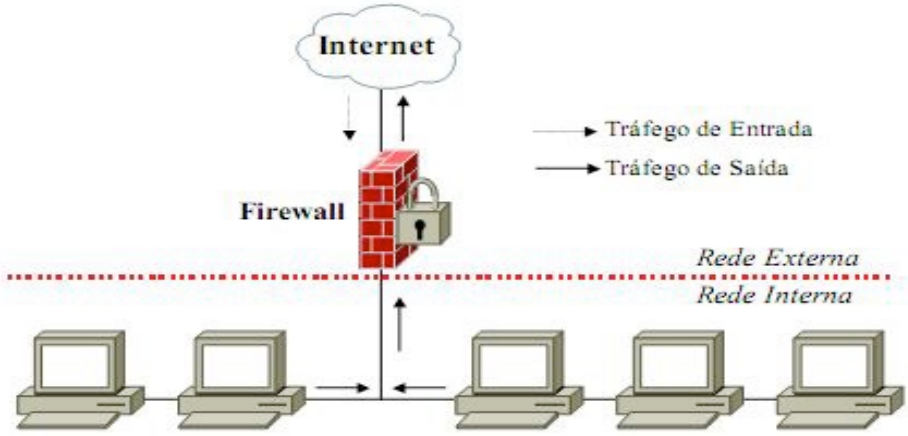

Figura - 2. A defesa é mais complexa do que o ataque
*Nota:*Fonte: Oliveira (2009, p.28).

Entretanto, na figura 2, pode-se analisar que a defesa é mais complexa que o ataque. Assim temos que estar preparados para impedir qualquer falha de segurança da informação, porque se formos atacados dificilmente conseguiremos nos defender do ataque. O termo *Hacker* ainda é muito discutido, mas preferimos usar o *Crack* por ter uma definição clara de criminoso virtual. Já o *Hacker* não necessariamente tem como prática um crime virtual, porém ambos possuem as mesmas capacidades, onde o *Hacker* vem na forma defensiva, e geralmente é contratado para proteger o sistema de segurança de uma empresa.

As formas de roubos informáticos são muito silenciosas e imprevisíveis. Por isso, a escolha de um método de segurança tem sido um grande desafio, devido a problemática em que vivemos. Enquanto uns estudam as formas de se proteger, outros passam muito tempo para farejar qualquer informação que permite-lhes cometer a fraude virtual, entretanto, as formas de ataque são várias, cada uma com a sua especificidade, cada caso é um caso, pelo que tem sido difícil detetar as reais falhas de segurança.

Oliveira (2009, p. 40) menciona, basicamente, os seguintes passos são executados por atacantes:

> Passo 1: O atacante, ao penetrar em sua rede, quebrando uma determinada máquina.
>
> Passo 2: Instala um programa *sniffer*.
>
> Passo 3: Este programa monitora a rede em busca de acesso a serviços de rede, as capturas são realizadas e registradas em um *log file*.
>
> Passo 4: Em seguida, o arquivo de *log* é recuperado pelo atacante.

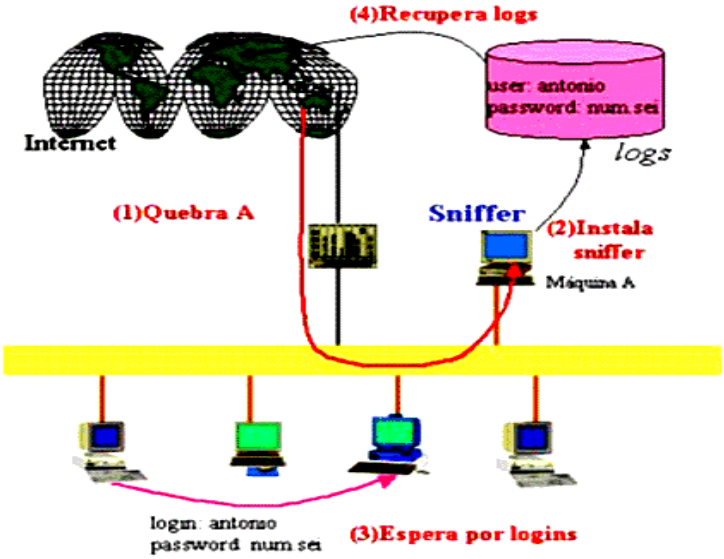

Figura - 3. Roubo de informações
*Nota:*Fonte: Oliveira (2009, p. 40)

As empresas corporativas atuais apresentam programas ou aplicativos informáticos para transferências bancárias, consultas de saldos, extração de extratos e diversos tipos de pagamentos *on-line*, essas tarefas que tornam alguns usuários vulneráveis por não possuírem educação de segurança, estas operações geralmente são feitas por dispositivos celulares que é utilizado por pessoas que podem ter acesso as credenciais, sem mencionar outras formas de crimes virtuais. As fraudes bancárias também são frequentes o envio de mensagens estranhas, ou via *e-mail* geralmente contendo *malware* ou *spyware* a exemplo disto podemos analisar o *Phishing*.

Implementação das medidas de segurança da informação

É importante ter formação básica de técnicas de segurança, as empresas têm que formar os seus funcionários para poder potenciar a segurança da informação.

Afirma Oliveira (2009, p. 10) "*Não adianta uma organização estar atuando virtualmente se as informações que alimentam o sistema estiverem vulneráveis. Da mesma forma que este é um fator diferencial para a globalização, a vulnerabilidade pode conduzir ao fracasso uma empresa*."

Algumas Práticas inseguras:

1. Abertura de email eletrónico suspeito;
2. Compras *on-line* com cartões de créditos em empresas não seguras;

3. Deixar ligado o *bluetooth* do seu celular;
4. Instalar softwares no celular em sites fora do *playstore, appstore, itunesstore e googlestore;*
5. Permitir que o seu dispositivo celular esteja desprotegido;
6. Permitir pessoas não autorizadas o acesso a suas credenciais;
7. Utilização de *sites* suspeitos;
8. Utilização do seu computador sem senha segura;
9. Utilização de publicidades enganosas;
10. Utilizar dispositivos de armazenamento em computadores infetados;
11. Utilizar partilha de multimídia de origem duvidosa;
12. Utilizar rede sem - fio desprotegida;
13. Utilizar um computador sem antivírus atualizado ou desprotegido;
14. Utilizar um servidor sem *antimalware, antispyware e firewall*.

Algumas empresas também possibilitam a falha da segurança, quer por parte de *hardware* ou software, mas abordaremos neste momento as falhas relacionadas com a parte lógica:

Falhas de segurança lógica nas empresas:

1. Permitir que *Crackers* monitoram as credenciais dos clientes;
2. Permitir a vulnerabilidade nos sistemas de segurança;
3. Permitir a clonagem de cartões de créditos dos clientes;
4. Permitir o vazamento de notícias e multimídia dos clientes;
5. Permitir a perda de dados e dossiers sigilosos dos clientes;
6. Permitir os desvios de dados bancários;
7. Permitir os desvios de fórmulas, patentes e protótipos;
8. Permitir alteração de dados académicos nas universidades.

Falhas de segurança física ou *hardware* que facilitam o crime virtual ou cibernético:

1. Permitir pessoas não autorizadas o acesso a sala de controle ou de segurança (engenharia social);
2. Permitir o acesso as câmaras de segurança;
3. Permitir o acesso ou roubo de dispositivos informáticos (Disco rígido, externos, *Pen-drive* e CDs) que contêm informações sigilosas;
4. Por falta de atenção permitir a utilização de caixas eletrónicas (ATM) com placas clonadas.

No entanto, para medidas de segurança da informação recomendamos o protocolo SET, segundo Gonsalez (2011):

> O protocolo SET, (*Secure Electronic Transaction*) é um protocolo criado com o objetivo de proporcionar segurança no tempo para fazer uma transação na internet, este protocolo foi criado única e exclusivamente para fazer transações eletrónicas seguras oferecendo serviços como:
>
> - Autenticação;
> - Confidencialidade;
> - Integridade;
> - Intimidade;
> - Verificação imediata;

- Não repúdio.

É sabido que existe muitas medidas para a segurança: preventiva, detetiva e corretiva.

As medidas preventivas

São medidas de precaução dos ataques informáticos. Por exemplo, aos servidores é aconselhável instalar firewall, utilizar técnicas criptográficas, colocar uma senha segura, criar *back-ups* ou cópias de segurança redundantes. Para os dispositivos informáticos como computadores orienta-se instalar antivírus completo com todos recursos, especialmente *antimalware, antispyware, antispam* e passar por um processo de atualização constante. No entanto o controle físico, deve-se instalar câmaras de vigilância, alarmes, contratar uma empresa de proteção física para o controle do espaço, contratar um *Hacker* para monitorar e testar os sistemas de segurança e sem esquecer a ação formativa dos técnicos sobre sistema de segurança.

As medidas detetivas

Essas medidas são necessárias quando se quer monitorar ou auditar a segurança na empresa ou exista um farejador de invasão de ataques. São medidas que podem ser realizadas com a presença do *Hacker* contratado para monitorar todos recursos e reportar a empresa o estado da segurança da mesma.

As medidas corretivas

Medidas deste género são preocupantes, mas o seu impacto é maior quando medidas anteriores não foram efetuadas na íntegra, apesar de afirmamos anteriormente que a questão de segurança é muito delicada, exige enormes investimentos que nem sempre as empresas estão preparadas financeiramente para suportar esta situação. São aquelas que acontecem de índole emergencial, sem ser planejadas, e prejudicam o ambiente das tecnologias de informação. Por isso, devem ser rapidamente resolvidas para a saúde da empresa. É necessário medir os riscos, porque as perdas de dados são muitas vezes irreparáveis, por essa razão o *Hacker* tem que avaliar os riscos que a empresa possui utilizando este ou aquele tipo de segurança, sabendo que até o momento não temos sistemas de segurança totalmente seguros.

Política de segurança e de contingência

Ameaça física

> São aquelas que os recursos materiais utilizados no ambiente de informação estão expostos, colocando em risco a integridade operacional da organização. Infelizmente, em muitas empresas, se gasta muito em segurança das informações e terminam se esquecendo de proteger o património (Oliveira, 2009, p. 15).

Segurança Física

A segurança física também é muito comum destaca-se os incêndios, as descargas elétricas, tempestades, problemas elétricos, mal uso de equipamento, acesso indevido à sala de segurança e ao centro de processamento de dados.

As medidas de segurança físicas são:

1. Colocar guardas no centro de controle;
2. Colocar portas com fechaduras;

3. Instalação de câmaras de vigilância;
4. Instalar alarmes transmitidos diretamente para o centro de controle policial;
5. Instalar extintores;
6. Instalar *firewall* físico;
7. Instalar sistemas de escutas;
8. Utilizar *No-Breaks*.

Segundo Oliveira (2009, p. 15):

Ameaça Lógica

"Ocorrem quando acontece uma modificação da capacidade funcional devido a dolo, acidente ou erro de recursos."

Segurança Lógica

A segurança lógica é mais abrangente:

1. Criptografia: é a arte de escrever e esconder códigos de forma a informação apresentar irreconhecível;
2. *Firewall*: tem a função permitir ou impedir pacotes. Sendo um dos fundamentais da segurança;
3. *Gateway* de circuitos: tem a função de permitir ou recusar através de um servidor *proxy* comandos específicos de certas aplicações, e operam na camada 4 do modelo OSI;
4. *Bastion Hosts*: são aqueles que os *hosts* antes de alcançarem a rede interna precisa passar primeiro ao *bastion hosts*, tendo ou não permissão;
5. *Behavior-Based Intrusion Detection*: é utilizado para desviar o normal comportamento do usuário;
6. Protocolo *Radius*: é um sistema de segurança cliente/servidor;
7. NAT - *Network AddressTranslation*: é utilizado para a economia de endereços IP;
8. Sistemas baseados na Rede (SDIR) ou *Network-Based Intrusion Detection System* (NIDS): também efetuam o monitoramento do tráfego da rede a partir dos cabeçalhos e conteúdos dos pacotes;
9. *Single Sign-On* (SSO): é um método que utiliza autenticação única e transparente, para diversos sistemas corporativos;
10. *Honey pot*: é muito utilizado para testar os sistemas de segurança, permitindo uma maior visibilidade do real estado da empresa, também é utilizado para preservar a rede de ataques;
11. Rede privada virtual (VPN): são responsáveis para garantir a autenticidade, privacidade, integridade dos dados, especialmente a tecnologia da criptografia;
12. *Kerberos*: possui uma chave secreta para cada usuário;
13. *Knowledge–Based Intrusion Detection*: os ataques são detetados como um antivírus;
14. Sistemas de deteção de intrusão (IDS): tem como objetivo monitorar e acompanhar a ação interna e externa da rede;

15. Escrever a URL no *browser*: permite utilizar de forma segura os *sites* credenciados;
16. DMZ - Zonas Desmilitarizadas: é uma rede intermediária composta com *firewall*, servidores e *switch*, que permanece entre a rede interna e externa.

Resultados

A pesquisa foi realizada com o intuito de propor medidas de segurança para as empresas corporativas do ramo da tecnologia de informação. Neste entendimento, foram propostas duas formas de proteção de segurança da informação: a lógica (*Software*) e Física (*Hardware*).

Mecanismos básicos de segurança devem ser estudados de forma profunda, como a identificação, autenticação, autorização, integridade, confidencialidade e disponibilidade.

Na atualidade, deve-se haver um olhar especial para as redes sociais, pois elas também permitem inúmeros ataques de vírus informáticos, espiões para cópias de credenciais, senha de utilizadores, códigos diversos, permitindo enviar para um computador remoto e, assim conceder ao *Crack* cometer o crime.

Destaca-se que, mesmo que sendo algo já muito estudado e difundido na literatura, o constante estudo e pesquisa na questão da segurança da informação ajuda na prevenção, reduzindo assim gastos económicos desnecessários com base nas medidas de segurança preventivas, que são medidas de precaução dos ataques informáticos, por exemplo aos servidores, aconselha-se instalar *firewall*, *antimalware*, *antispyware* e utilizar técnicas criptográficas, colocar uma senha segura, criar *back-ups* ou cópias de segurança redundantes.

Quanto as medidas detetiva são necessárias quando se quer monitorar ou auditar a segurança nas empresas ou exista um farejador de invasão de ataques. São medidas que podem ser realizadas com a presença do *Hacker* contratado para monitorar todos recursos e reportar a empresa o estado da segurança da mesma.

Já no tocante as medidas corretivas é preocupante, mas o seu impacto é maior quando medidas anteriores não forem efetuadas na íntegra. Por fim, orienta-se que de forma generalizada, se tenham um plano de contingência para impedir os ataques nas empresas corporativas para que se implemente todas as medidas propostas.

Conclusão

Os ataques cibernéticos têm trazido muitas dificuldades, os *malwares* são pertencentes a vários grupos dos vírus informáticos, exemplo o *trajon, worms* ou vermes, *dropper*, e *backdoor*, estão na base de muitas perdas económicas, a falsa identidade, a espionagem o roubo de dados, os tipos de fraudes informáticos e o envio de dados para um computador remoto, mesmo que esteja geograficamente distantes ou em continentes diferentes.

As perdas económicas originadas por falhas na segurança da informação, tem tornado um escândalo que envolve grandes figuras do mundo. No entanto os golpes de estados, as fraudes eleitorais, vazamento de informação política, segredos de estado e desvios bancários têm preocupado todas nações, entretanto politicas para criar legislação para punir os criminosos virtuais é a melhor saída. Estes casos despertou a comunidade internacional as empresas os governos virar as intenções sobre a segurança da informação que era uma preocupação nacional que passou ser a problemática mundial.

Quanto a estes ataques a empresas, sabe-se que eles são mais expressivos por *Crackers* ou *Hackers*, e um número menos representativos de antigos funcionários. Para isso, orienta-se que medidas de segurança preventiva, detetiva e corretiva sejam usadas dentro de um plano de segurança e de contingência.

As medidas de segurança identificadas e propostas se embaçam em física e lógica. Sendo para controle da segurança física orienta-se a especial atenção ao ambiente físico da organização.

Já quanto a segurança lógica, que é mais abrangente, especialmente para segurança da informação para as empresas corporativas, tem-se como sugestão o emprego da criptografia, o uso de *firewall* permitindo ou impedindo a entrada ou saída de pacotes de dados importantes.

Referências

CERT.br. (2012). *Cartilha de Segurança para Internet*: *Interceptação de tráfego* (Sniffing). 4.0-Versão. São Paulo. Disponível em: http://cartilha.cert.br/.

Coopamootoo, K. (2018). *Cyber Security*: *Privacidade online e offline.* [vídeo]. Newcastle University. Retrieved from: https://www.futurelearn.com/courses/cyber-security/0/steps/19596.

Creswell, J. W. (2010) Projeto de pesquisa métodos qualitativo, quantitativo e misto. In: Projeto de pesquisa métodos qualitativo, quantitativo e misto.

Financial Fraud Action UK. (2017). *Fraud The Facts: This category covers fraud on cards that have been.* Retrieved from: https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf.

Futurelearn. (2018a). *Cyber Security: Riscos pessoais decorrentes de violação de privacidade nos negócios.* [vídeo]. Newcastle University. Retrieved from:https://www.futurelearn.com/courses/cyber-security/0/steps/19598.

Futurelearn (2018b) *Cyber Security for Small and Medium Enterprises: What can we learn from this attack?* Universidade Deakin. Retrieved from: https://www.futurelearn.com/courses/cyber-security-business#what-is-upgrade.

Gonsalez. Y. J. (2011) *Que es Protocolo SET*. Universidad de le Salle. Retrievedfrom:https://www.researchgate.net/publication/261551164_QUE_ES_PROTOCOLO_SET

Martinelli, H. (2008). *Vírus de Celular: Estudo e classificação para um protótipo de defesa: O início das ameaças: Quanto às formas de propagação mais comuns temos*. Uniritter. Brasil - RS, Porto Alegre.

Laureano, M. A. P. (2005) *Gestão de segurança da informação.* Retrieved from: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf.

Oficina da Net. (2015) *Samsung é condenada a pagar indemnização milionária a Apple*. Retrieved from: https://www.oficinadanet.com.br/post/14544-samsung-e-condenada-a-pagar-indenizacao-milionaria-a-apple.

Oliveira, G. (2009). *Segurança de redes: As ameaças organizacionais.* Escola Superior Aberta do Brasil - Vitoria - Espírito Santo.

Quissanga, F. C. (2015).*Caracterização de vírus informáticos em telefonia móvel celular: Propagação e infecção.* (Trabalho de conclusão do curso) Escola Superior Aberta do Brasil -ESAB - Vitoria - Espírito Santo.

Portal de periódicos capes. Missão e Objetivos. Disponível em: https://www.periodicos.capes.gov.br/index.php?option=com_pcontent&view=pcontent&alias=missao-objetivos&Itemid=144.

Terra (2016). Panama Papers. Retrieved from: https://www.terra.com.br/noticias/mundo/panama-papers-geram-denuncias-e-investigacoes-em-todo-o mundo,814039f797239995dea030884e41f8faakajlviv.html.

Fecha de envío:14/03/2020
Fecha de revisión:14/04/2020
Fecha de aceptación: 02/06/2020