CENTRO PAULA SOUZA
GOVERNO DE SÃO PAULO
FACULDADE DE TECNOLOGIA
DE SÃO CAETANO DO SUL

ALESSANDRO SIQUEIRA E SILVA
KARINA FLAMINO LUGARINI SILVA
PÂMELA SOARES LORENÇÃO
SÉRGIO DA SILVA BARROS

Estudo de Vulnerabilidades em Sistemas de Videomonitoramento

São Caetano do Sul – SP
2020

ALESSANDRO SIQUEIRA E SILVA

KARINA FLAMINO LUGARINI SILVA

PÂMELA SOARES LORENÇÃO

SÉRGIO DA SILVA BARROS

Estudo de Vulnerabilidades em Sistemas de Videomonitoramento

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de São Caetano do Sul, sob a orientação do Professor Me. Kleber da Silva Divino, como requisito parcial para a obtenção do diploma de Graduação no Curso de Segurança da Informação.

São Caetano do Sul - SP

2020

FACULDADE DE TECNOLOGIA DE SÃO CAETANO DO SUL

ALESSANDRO SIQUEIRA E SILVA
KARINA FLAMINO LUGARINI SILVA
PÂMELA SOARES LORENÇÃO
SÉRGIO DA SILVA BARROS

Estudo de Vulnerabilidades em Sistemas de Videomonitoramento

BANCA EXAMINADORA

_____
Prof.Me. Kléber da Silva Divino - Orientador

Prof. _____
Instituição: _____
Julgamento: _____

Prof. _____
Instituição: _____
Julgamento: _____

AGRADECIMENTOS

Nossos primeiros agradecimentos irão para Deus, por nos proporcionar sabedoria, discernimento, paciência e saúde para concluirmos essa etapa tão importante de nossas vidas.

Agradecemos aos nossos pais, estejam eles aqui ou no plano espiritual, por serem a nossa base e por nos darem o apoio necessário durante todo o nosso processo de formação como pessoas e profissionais.

Nossos sinceros agradecimentos ao nosso orientador Kléber da Silva Divino por todo apoio, por acreditar em nosso trabalho e dedicação na elaboração do nosso trabalho.

Agradecemos também todo corpo docente e de colaboradores da Fatec São Caetano pelo carinho, respeito e incentivo a nós dispensados.

E aos nossos colegas por todo apoio.

RESUMO

BARROS, S. S.; LORENÇÃO, P. S.; SILVA, A. S. E; SILVA, K. F. L. **Análise de vulnerabilidades em sistemas de vigilância pública**. Trabalho de Graduação – Faculdade de Tecnologia Antônio Russo, São Caetano do Sul, 2020.

Zelar pela segurança da população tornou-se algo primordial em grandes centros urbanos, e para tal algumas cidades instalam sistema de videomonitoramento, ou seja, câmeras em vias públicas.

Devido ao baixo custo e à grande demanda na procura desses equipamentos, muitos fabricantes não se atentam à segurança dos seus equipamentos expondo as suas vulnerabilidades, permitindo pessoas mal intencionadas a ter acesso a informações privilegiadas e confidenciais, ferindo, assim, os pilares da segurança da informação: Confidencialidade, Integridade e Disponibilidade.

Pensando nessas falhas de segurança, dedicamos a nossa pesquisa às principais vulnerabilidades dos equipamentos que compõem o sistema de videomonitoramento. A partir dessa identificação, propusemos formas de mitigar os riscos, e montamos um *check list*, objeto principal do nosso trabalho.

Este estudo é direcionado aos responsáveis pela decisão de implementar novos sistemas de videomonitoramento nas áreas urbanas.

Palavras - chave: segurança da informação, vulnerabilidade, videomonitoramento

ABSTRACT

BARROS, S. S.; LORENÇÃO, P. S.; SILVA, A. S. E; SILVA, K. F. L. **Analysis of vulnerabilities in public surveillance systems**. Final Paper – Faculdade de Tecnologia Antônio Russo, São Caetano do Sul, 2020.

Ensuring the safety of the population has become paramount in large urban centers, therefore cities have been installing video surveillance systems, that is, cameras on public roads.

Due to the low cost and the great demand in the search for this equipment, many manufacturers do not pay attention to the security of their equipment, exposing their vulnerabilities, giving malicious users access to privileged and confidential information, thus attacking the pillars of information security: Confidentiality, Integrity and Availability.

Focusing on these security flaws, we dedicated our research to the main vulnerabilities of the equipment that make up the video monitoring system. Based on this identification, we proposed ways to mitigate risks, as welle as setting up a check list, the main object of our work.

This study addresses to those responsible for deciding to implement new video surveillance systems in urban areas.

Keywords: information security, vulnerability, video monitoring

LISTA DE FIGURAS

Figura 1: Mapeamento de Câmeras 12
Figura 2: Comunicação das camadas do Modelo OSI 15
Figura 3: Comunicação TCP/IP 17
Figura 4: Componentes básicos de CFTV 25
Figura 5: Câmera Panorâmica e Domo 26
Figura 6: Diagrama da Botnet 33
Figura 7: Diagrama do Mirai 35
Figura 8: Diagrama de Criptografia Simétrica 40

LISTA DE QUADROS

Quadro 1 Análise de Vulnerabilidades 41

LISTA DE ABREVIATURAS E SIGLAS

CCD	Charged Coupled Device
CFTV	Circuito Fechado de Televisão
CID	Confidencialidade, Integridade e Disponibilidade
CIF	Common Interchange Format
COI	Centro de Operações Integradas
COR	Centro de Operações Rio
CONSEG	Conselho Comunitário de Segurança
CRT	Cathode Ray Tube
CVE	Common Vulnerabilities and Exposures
DSL	Digital Subscriber Line
DVR	Digital Video Recorder
HTTP	Hyper Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Internet Service Providers
JOSM	Java Open Street Map
LCD	Liquid Crystal Displays
MPEG	Moving Pictures Experts Group
NVR	Network Video Recorder
OSI	Open System Interconnection
OSM	Open Street Map
OWASP	Open Web Application Security Project
PC	Personal Computer
PD	Powered Device
PSE	Power Sourcing Equipments
PTZ	Pan Tilt Zoom
PoE	Power Over Ethernet
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RTSP	Real Time Streaming Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

UTP	Unshield Twisted Pair
VHS	Video Home System
VMS	Video Management Software

SUMÁRIO

INTRODUÇÃO 10
1. REDES DE COMPUTADORES 13
1.1. Estrutura do Modelo *Open System Interconnection* (OSI) 14
1.2. Protocolos 16
1.2.1. Protocolo TCP/IP 16
1.2.2. Protocolo HTTP e HTTPS 18
1.2.3. Protocolo RTSP 19
1.3. Meios de Transmissão/Conexões 20
1.3.1. Cabos 20
1.3.2. Fibra Ótica 21
1.3.3. Wireless Fidelity (Wi-Fi) 21
1.3.4. *Power Over Ethernet* (PoE) e PoE + ... 22
2. VIDEOMONITORAMENTO 24
2.1. Circuito Fechado de Televisão (CFTV) 24
2.2. Tipos de Câmeras 25
2.3. Video Management System (VMS) 26
2.4. Digital Video Recorder (DVR) 27
2.5. Network Video Recorder (NVR) 28
2.6. Codificadores/Decodificadores de Vídeos (CODECs) 28
2.7. Firmware 29
3. SEGURANÇA DA INFORMAÇÃO 30
3.1. Vulnerabilidades 30
3.2. Malware 31
3.3. Botnet 33
3.4. Mirai 34

4. VULNERABILIDADES EM CFTV 36
4.1. Vulnerabilidades em Câmera de videomonitoramento 37
4.2. Vulnerabilidades em protocolos de transmissão 38
4.3. Vulnerabilidades em meios de armazenamento 38
4.4. Vulnerabilidades Físicas 39
4.5. Criptografia 39
4.6. Mitigação das Vulnerabilidades 40
4.7. Checklist 42
5. CONSIDERAÇÕES FINAIS 43
APÊNDICE A 48
APÊNDICE B 49

INTRODUÇÃO

Após 11 de Setembro de 2001, medidas de segurança vêm sendo cada vez mais exploradas, e uma dessas medidas é o videomonitoramento. Esse sistema de vigilância foi utilizado e continua sendo em países considerados grandes potências mundiais, e em outros menos favorecidos, com o intuito de reduzir ameaças terroristas e de inibir a criminalidade nas áreas urbanas.

Como trata-se de uma tecnologia de baixo custo, isso foi um facilitador para a implantação desse sistema em nosso cotidiano. Muitas vezes estamos sendo monitorados em espaços urbanos e nem percebemos.

Mas como esse método de segurança funciona? É um sistema informatizado? Será que está suscetível a vulnerabilidades em alguma parte do processo, seja nas partes físicas (*hardware*), transmissão (redes sem fio, cabos e fibras óticas), ou na parte lógica (criptografia e *softwares*) e processos?

Segundo Laudon (2007), ao operar uma empresa, atualmente é necessário apresentar segurança compreendendo aqui políticas, procedimentos e medidas técnicas usadas para impedir acesso não autorizado, alteração, roubo ou danos físicos aos sistemas. Também proporcionar controle, por sua vez, incidindo em todos os métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis e a adesão operacional aos padrões administrativos.

A partir de uma pesquisa feita em determinada região, que utiliza o serviço de videomonitoramento nas vias urbana e em visita feita ao centro de controle das imagens, identificamos algumas vulnerabilidades que podem colocar em risco e expor as pessoas que estão sendo monitoras, bem como todo o processo dos serviços envolvidos.

Alguns sistemas de videomonitoramento são utilizados em espaços públicos para auxiliar as autoridades a minimizar ou inibir a criminalidade, mas será que esses sistemas têm a segurança necessária a fim de evitar que as imagens caiam em mãos de pessoas não autorizadas e que possam explorar as vulnerabilidades? É possível desenvolver uma metodologia para analisar e tratar as vulnerabilidades em sistemas de videomonitoramento?

Segundo a Cartilha de Segurança do Comitê Gestor da Internet no Brasil (2012), uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

Com base nos questionamentos e nessa definição, e à medida em que a implantação de circuitos de segurança crescem nos centros urbanos, resolvemos analisar algumas das vulnerabilidades que este sistema pode apresentar, e a partir dessa análise elaborarmos um *check list* (objeto principal da nossa pesquisa), onde apontamos o que deve ser verificado antes de novos sistemas serem implantados, a fim de proteger o sistema contra pessoas mal intencionadas, e também garantir que os pilares da Segurança da Informação: Confidencialidade, Integridade e Disponibilidade (CID), não sejam afetados.

Nosso trabalho consistiu na elaboração de uma pesquisa bibliográfica no âmbito do sistema de videomonitoramento em vias públicas, com o intuito de conhecer as principais vulnerabilidades envolvidas nos sistemas em questão, levantar as ferramentas necessárias para que sejam efetuados os testes para comprovar tais vulnerabilidades com a finalidade de corrigi-las.

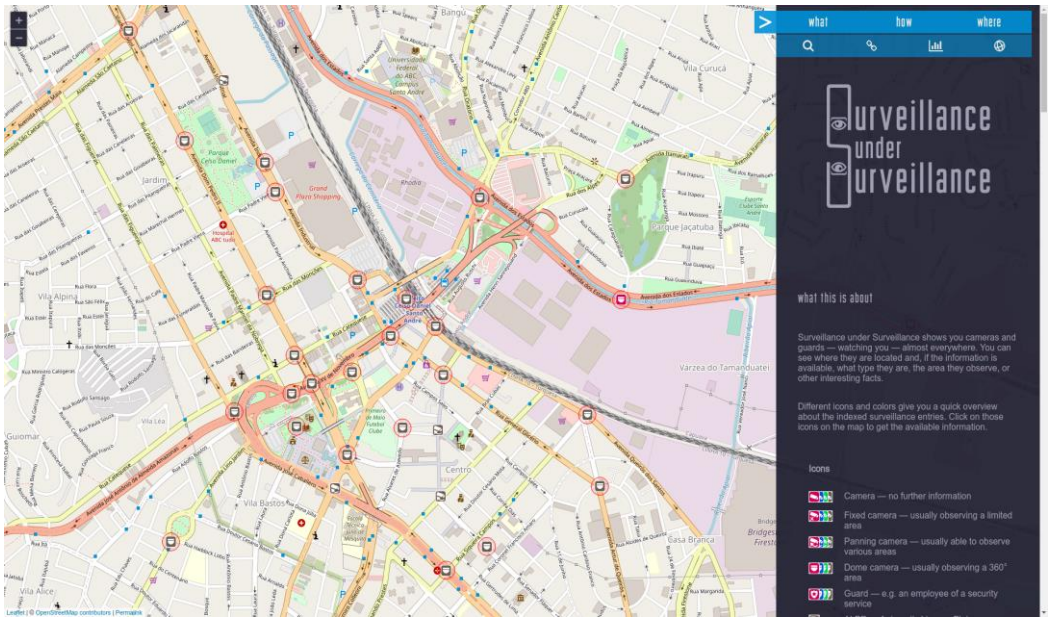
Além disso, percorremos as ruas de determinados bairros da região pesquisada, e realizamos manualmente o levantamento de dados (esses dados podem ser observados no Apêndice B), como: quantidade de câmeras, tipos de câmeras utilizadas, marca, modelo etc., para que assim obtivéssemos riqueza de detalhes e elaborássemos a nossa pesquisa da melhor forma para alcançarmos o nosso objetivo, que é contribuir com a melhoria da segurança de videomonitoramento em vias públicas através da elaboração de um *check list*.

Inserimos os pontos administrados pelo poder público localizados no *Open Street Map* (OSM), que é um mapa *online* colaborativo de código aberto, onde há diversas “derivações” como o *Surveillance Under Surveillance* 7 (Figura 1), que é um mapa online focado em vigilância pública, onde além da localização geográfica, ainda podem ser colocados vários detalhes das câmeras, como por exemplo: o link quando a câmera tem acesso público[1].

---

[1] Mais detalhes do mapeamento e inserção de câmeras no *OpenStreetMap* e *Surveillance Under Surveillance* estão disponíveis em: https://sickeira.blogspot.com/2020/06/open-street-map-cameras-no-osm.html.

Figura 1: Mapeamento de Câmeras



Fonte: Autoria Nossa

Para que o *check list* fosse efetivo, foi necessário conhecermos como e onde as imagens das câmeras de segurança são armazenadas, identificarmos as vulnerabilidades mais críticas ao sistema, bem como entender todo o funcionamento do processo de videomonitoramento público, visando a correção das falhas e com isso a mitigação dos riscos e a redução à exposição de dados sensíveis, para que este possa ser utilizado na implantação de qualquer tipo de sistema de monitoramento de vias urbanas.

É de suma importância que os usuários dos sistemas de videomonitoramento saibam como funciona a transmissão das informações, então para efeito de conhecimento e orientação, descrevemos a seguir capítulos referentes a redes, meios de armazenamento, meios de transmissão, vulnerabilidades, bem como os principais itens que devem ser observados e checados ao implementar esse tipo de sistema.

1. REDES DE COMPUTADORES

Uma rede de computadores é uma conexão entre dois ou mais dispositivos de *hardware* ligados entre si por canais de comunicação que facilitam a comunicação e o compartilhamento de recursos entre uma ampla gama de usuários.

Segundo Fourozan (2008), a internet é um conjunto de redes remotas (eixos centrais), comutadas, rede locais, redes remotas ponto a ponto e dispositivos de conexão.

A internet hoje é o maior sistema de engenharia já criado pela humanidade, com centenas de computadores conectados; bilhões de usuários que se conectam por meio de laptops, tablets e smartphones; e com uma série de dispositivos como sensores, webcams, console para jogos, e até mesmo máquinas de lavar sendo conectadas. Dado que a Internet é tão ampla e possui inúmeros componentes e utilidades. (KUROSE; ROSS, 2013).

Cada vez mais sistemas finais modernos como automóveis, sistemas internos elétricos e de segurança, estão sendo conectados à rede. Todos esses equipamentos são denominados hospedeiros ou sistemas finais. (KUROSE; ROSS, 2013).

Sistemas finais são conectados entre si por enlaces (*links*) de comunicação e comutadores (*switches*) de pacotes. Há muitos tipos de enlaces de comunicação, que são constituídos de diferentes tipos de meios físicos, entre eles cabos coaxiais, fios de cobre, fibras ópticas e ondas de rádio. (KUROSE; ROSS, 2013).

As redes locais ou remotas normalmente não funcionam isoladamente. Elas são conectadas umas às outras ou à internet. Para conectar redes locais ou remotas usamos dispositivos de conexão. Os dispositivos mais conhecidos são os roteadores e comutadores de camada de enlaces. Esses encaminham os pacotes de informações a seus destinos. (FOROUZAN, 2008).

A sequência de enlaces de comunicação e comutadores de pacotes que os pacotes percorrem desde o sistema final remetente até o sistema final receptor é conhecido como rota ou caminho através da rede. (KUROSE; ROSS, 2013).

Sistemas finais acessam a Internet por meio de Provedores de Serviços de Internet (*Internet Service Providers – ISPs*). ISPs oferecem aos sistemas finais uma variedade de tipos de acesso à rede, incluindo acesso residencial de banda larga como modem a cabo ou *Digital Subscriber Line (DSL)*, acesso por uma *Local Area Network* (LAN) de alta velocidade, acesso sem fio e acesso por modem discado, além

de fornecerem também acesso a provedores de conteúdo, conectando sites diretamente à Internet. (KUROSE; ROSS, 2013).

1.1. Estrutura do Modelo *Open System Interconnection* (OSI)

Com a complexidade do mundo de hoje, a maioria das empresas possui redes, e estão presentes na *Web.* Uma rede pode variar desde simplesmente dois computadores ligados até a complexidade dos computadores que podem acessar dados entre continentes (BARRETT, KING, 2010).

Ao se comunicarem, os computadores compartilham recursos que podem ser: dados (documentos ou planilhas), aplicações (Editor de texto ou Planilha eletrônica), *hardware* (modems ou impressoras), etc.

Quando o uso de redes se tornou a norma para as empresas, surgiu a necessidade de que estas pudessem se conectar, embora seus equipamentos e sistemas fossem diferentes. (BARRETT, KING, 2010).

A *International Standards Organization* (ISO), órgão que se dedica ao estabelecimento de acordos mundiais sobre padrões internacionais, em 1978 desenvolveu uma arquitetura que permitiria a comunicação entre dispositivos de diferentes fabricantes, e entre todos os tipos de sistema de computadores. Esse modelo de referência ficou conhecido como modelo de Interconexão de Sistemas Abertos ou *Open System Interconnection* (OSI).

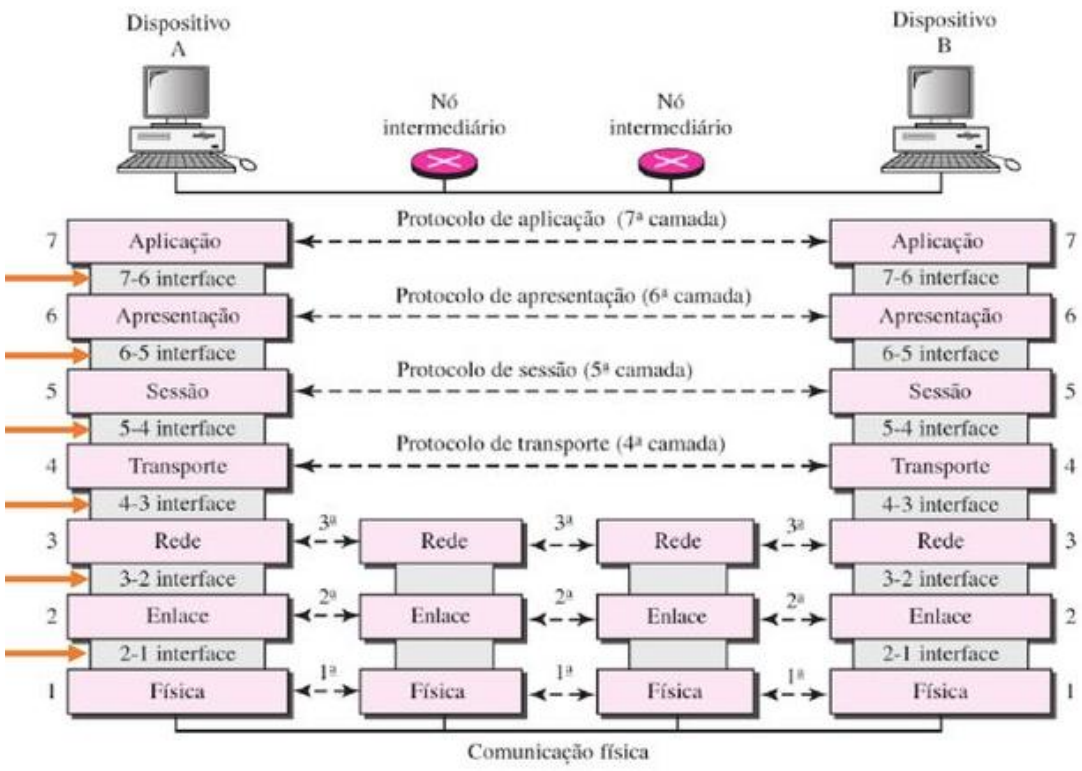
O modelo OSI não é um protocolo. O objetivo do modelo OSI é mostrar que é possível facilitar a comunicação entre sistemas diferentes. (FOUROZAN,2008).

Trata-se de um modelo baseado em sete camadas separadas, porém relacionadas:

- Aplicação
- Apresentação
- Sessão
- Transporte
- Rede
- Enlace de dados
- Física

Cada camada acrescenta funcionalidade à camada anterior e se comunica com as camadas diretamente acima e abaixo dela, como mostra a Figura 2.

Figura 2: Comunicação das camadas do Modelo OSI



Fonte: Forouzan, 2008.

O modelo OSI oferece um arcabouço conceitual para a comunicação entre os computadores, mas ele não é um método de comunicação entre si. A comunicação entre as máquinas são processos não hierárquicos, que utiliza protocolos adequados para determinada camada. A comunicação ocorre usando-se protocolos de comunicação, que são um conjunto de regras e convenções que controla as informações por meio de rede. (BARRETT; KING, 2010).

As sete camadas do modelo OSI podem ser divididas em duas categorias: Camadas superiores e camadas inferiores. As camadas superiores (5,6 e 7) podem ser consideradas como camadas de suporte de usuários e geralmente são implantadas somente em software. As camadas inferiores (1,2 e 3) são as de suporte de redes; lidam com os aspectos físicos de movimentação de dados de um dispositivo ao outro e podem ser implementadas em software e hardware, exceto a camada física, que é principalmente em hardware. A camada 4, de transporte, une os dois subgrupos

e garante que o conteúdo enviado pelas camadas inferiores possa ser usado pelas camadas superiores. (FOROUZAN, 2008).

1.2. Protocolos

Os sistemas finais, os comutadores de pacotes e outras peças da Internet executam protocolos que controlam o envio e o recebimento de informações. Os principais protocolos da Internet são *Transmission Control Protocol* (TCP) e *Internet Protocol* (IP) também conhecidos como protocolos TCP/IP. (KUROSE; ROSS, 2013).

Nas redes de computadores, como a comunicação ocorre entre entidades de diferentes sistemas, para que a comunicação ocorra, as entidades devem estar de acordo com um protocolo. Um protocolo é um conjunto de regras que governa a comunicação de dados. Um protocolo define o que é comunicado, como é comunicado e quando. (FOROUZAN, 2008).

Para uma melhor compreensão, KUROSE e ROSS (2013) fizeram uma analogia com a comunicação humana, uma vez que executamos protocolos o tempo todo. Se as pessoas executarem protocolos diferentes (por exemplo, se uma pessoa tem boas maneiras, mas a outra não), os protocolos não interagem e nenhum trabalho útil pode ser realizado. O mesmo ocorre com as redes. É preciso que duas (ou mais) entidades comunicantes executem o mesmo protocolo para que uma tarefa seja realizada.

1.2.1. Protocolo TCP/IP

O protocolo TCP fornece serviços de camadas de transporte completos para os aplicativos. É um protocolo de transporte de fluxo confiável.

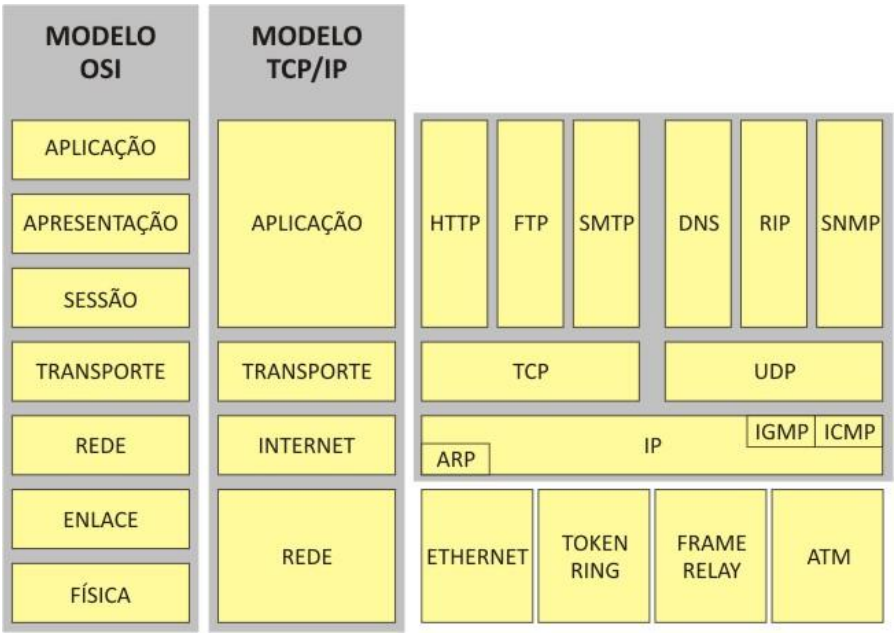
Já o IP é um mecanismo de transmissão usado pelos protocolos TCP/IP. É um protocolo não confiável e sem conexão – um serviço de envio pelo melhor esforço (não verifica ou controla erros). Faz o possível para que a transmissão chegue ao seu destino, mas sem garantia. (FOROUZAN, 2008).

O sistema de comunicação de dados é formado por cinco componentes: mensagem, receptor, emissor, meio de transmissão e protocolo.

O protocolo representa um acordo entre os dispositivos de comunicação. Sem um protocolo, dois dispositivos podem ser conectados, mas sem se comunicar. (FOROUZAN, 2008).

O conjunto de protocolos TCP/IP foi desenvolvido antes do modelo OSI, portanto, as camadas não correspondem. É composto de cinco camadas: física, enlace de dados, rede, transporte e aplicativo.

Figura 3: Comunicação TCP/IP



Fonte: Reis, 2017.

A comunicação entre os dados pode ser: *Simplex* (só envia); *Half- Duplex* (num instante envia e no outro instante recebe) ou *Full Duplex* (envia e recebe ao mesmo tempo). (FOROUZAN, 2008).

Enquanto o modelo OSI especifica quais funções pertencem a cada uma de suas camadas, as camadas do conjunto de protocolos TCP/IP contêm protocolos relativamente independentes que podem ser misturados e combinados de acordo com as necessidades do sistema. (FOROUZAN, 2008).

A função da camada de transporte é aceitar dados da camada acima dela, dividi-los em unidades menores caso necessário, repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade, além de determinar que tipo de serviço deve ser fornecido à camada de sessão e, em última análise, aos usuários da rede (TANENBAUM, 2003).

O TCP é um protocolo de fluxo confiável, ou seja, orientado a conexão e oferece controle de fluxo de erro. Ele verifica se os dados são entregues com precisão e na sequência apropriada. (TANENBAUM, 2003).

O IP é um protocolo de encaminhamento, responsável por tornar os pacotes de dados roteáveis, sem conexão e não confiável. Não verifica ou controla erros (protocolo de melhor esforço). (FOROUZAN, 2008).

O TCP/IP usa um endereço de 32 bits no formato xxx.xxx.xxx.xxx. Cada xxx é chamado de octeto. Os endereços IPs são classificados em cinco classes: (BARRETT, KING,2010).

- Classe A: Pode aceitar uma rede com 16.777.216 hosts e tem o primeiro octeto entre 1 e 126.
- Classe B: Pode aceitar 65.536 *hosts*[2] e tem o primeiro octeto entre 128 a 191.
- Classe C: Pode aceitar 254 *hosts* por rede e tem o primeiro octeto entre 192 e 223.
- Classe D: Reservada para envio de mensagens de *multicast*[3]. Começa com 224 e termina em 239.
- Classe E: Reservada para uso experimental. Começa com 240 e termina com 255.

O endereço IP 127.0.0.1 é o endereço de *loopback*[4], utilizado para diagnóstico.

1.2.2. Protocolo HTTP e HTTPS

O protocolo *Hyper text transfer protocol* (HTTP) é um protocolo da camada de aplicação, e com certeza um dos mais conhecidos quando o quesito é acesso a informações que estão na Internet. O HTTP trabalha na arquitetura de cliente-servidor, onde para executar as comunicações o cliente envia as mensagens de HTTP para o servidor e o modo de como essas mensagens serão respondidas. A comunicação é

---

2 *host* é qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos.

3 é um método ou técnica de transmissão de um pacote de dados para múltiplos destinos ao mesmo tempo.

4 é o endereço do próprio computador, ele é uma interface de rede virtual na qual um cliente e um servidor no mesmo host podem se comunicar entre si usando a pilha de protocolos TCP/IP, assim como permite também a verificação do funcionamento da camada TCP/IP.

feita de forma padronizada e todos os clientes e servidores atuam dessa forma utilizando o protocolo (KUROSE, ROSS, 2013).

Segundo Tanenbaum (2002), o modo habitual de um navegador entrar em contato com um servidor é estabelecer uma conexão TCP para a porta 80 da máquina servidora, embora esse procedimento não seja exigido formalmente. A vantagem de se usar o TCP é que este protocolo controla o fluxo mensagens perdidas, mensagens duplicadas, mensagens longas e confirmações.

O HTTP, protocolo de camada de aplicação da Web, define o formato e a sequência das mensagens que são passadas entre o navegador e o servidor. (KUROSE; ROSS, 2013).

1.2.3. Protocolo RTSP

O protocolo *Real Time Streaming Protocol* (RTSP), é executado na camada de aplicação, e permite o gerenciamento em tempo real, um ou vários fluxos de mídia de áudio e vídeo diferentes, ou seja, ele atua como uma ferramenta que permite controle remoto de serviços de multimídia permitindo o controle eficaz do monitoramento de circuitos de câmeras. (RAO et al., 2016).

O RTSP é um protocolo que foi intencionalmente desenvolvido para funcionar de maneira similar ao HTTP.

O protocolo possui as seguintes características:

- Extensível - existe a possibilidade de adicionar novos métodos de uso e novos parâmetros necessários ao RTSP.
- Fácil de analisar - o RTSP pode ser analisado pelos analisadores de HTTP comuns.
- Segurança - o RTSP é capaz de utilizar recursos de segurança disponíveis na web. As funções de autenticação HTTP. Pode-se também reutilizar a segurança do transporte ou da camada de rede.
- Confiabilidade de entrega - o RTSP pode usar um protocolo de datagrama não confiável conhecido como *User Datagram Protocol* (UDP), o protocolo confiável RDP, que não é amplamente utilizado ou um protocolo de fluxo confiável como o TCP, pois implementa a confiabilidade no nível da camada de aplicação.

- Capacidade para diversos servidores diferentes - Cada fluxo de mídia em uma apresentação pode estar alocado em um servidor diferente. O cliente estabelece automaticamente várias sessões de controle simultâneas com os diferentes servidores de mídia. A sincronização de mídia é realizada no nível da camada de transporte.
- Possibilidade de gravação - o protocolo pode controlar os dispositivos que operam a gravação e reprodução, e dispositivos que podem operar dos dois modos. (RAO et al., 2016).

1.3. Meios de Transmissão/Conexões

Um meio de transmissão, em termos gerais, pode ser definido como qualquer coisa capaz de transportar informações de uma origem a um destino, como, um espaço livre, um cabo metálico ou um cabo de fibra óptica. (FOROUZAN, 2007).

Os meios de transmissão são divididos em duas categorias: guiados e não guiados. Entre meios de transmissão guiados temos: cabos de par transado, cabos coaxiais e cabos de fibra óptica. Meios de transmissão guiados são aqueles que requerem um condutor físico para interligar um dispositivo a outro. (FOROUZAN, 2007).

Nos meios não guiados, as ondas se propagam na atmosfera e no espaço, como é o caso de uma LAN sem fio ou de um canal digital de satélite. (KUROSE; ROSS, 2013).

A transmissão das informações também acontece entre redes. As redes de acesso são usadas em ambientes domésticos, corporativos e móvel sem fio. Os dois tipos de acesso residencial são: a linha digital de assinante (DSL) ou a cabo. O acesso DSL à Internet é obtido da mesma empresa que fornece acesso telefônico local com fio, ou seja, a operadora local. Sendo assim, a operadora local também passa a ser seu provedor de Internet (ISP). (KUROSE; ROSS, 2013).

1.3.1. Cabos

Um dos meios de transmissão mais usados e de menor custo é o par de fio de cobre trançado. Este tipo de cabo vem sendo utilizado há anos em redes de telefonia. Cabos de par trançados e coaxiais usam condutores metálicos (cobre) que aceitam e transportam sinais na forma de corrente elétrica. (KUROUSE; ROSS, 2013).

Os fios são trançados para reduzir a interferência elétrica de pares semelhantes que estejam próximos. Um par de fios constitui um único enlace de comunicação. O par trançado sem blindagem U*nshielded Twisted Pair* (UTP) costuma ser usado em redes de computadores de edifícios, isto é, em LANs. Uma solução dominante para LANs de alta velocidade. O par trançado também é usado para acesso residencial à Internet. (KUROUSE; ROSS, 2013).

O cabo coaxial tem melhor blindagem que o par trançado. Comumente utilizado em transmissões digitais, analógicas e TV à cabo. Eram muito utilizados em linhas telefônicas de longa distância, mas atualmente estão sendo substituídos por fibras ópticas. (TANENBAUM, 2013).

1.3.2. Fibra Ótica

As Fibras óticas são imunes à interferência eletromagnética, têm baixíssima atenuação de sinal até cem quilômetros e são muito difíceis de derivar. Essas características fizeram da fibra ótica o meio preferido para a transmissão guiada de grande alcance, em especial para cabos submarinos. Muitas redes telefônicas de longa distância usam exclusivamente fibras óticas, que também predominam no *backbone*[5] da Internet. Contudo, o alto custo de equipamentos ópticos — como transmissores, receptores e comutadores — vem impedindo sua utilização para transporte a curta distância, como em LANs ou em redes de acesso residenciais. (FOROUZAN,2007).

1.3.3. Wireless Fidelity (Wi-Fi)

Embora muitas tecnologias para redes locais sem fios tenham sido desenvolvidas na década de 90, atualmente esse tipo de rede é uma das tecnologias mais importantes de acesso à internet. Tornou-se tão comum que estão presentes em todos os lugares: bares, restaurantes, aeroportos, escolas, empresas etc. Muitos aparelhos e eletrônicos já saem da fábrica com a possibilidade de comunicação via Wi-Fi. (DANTAS, 2010).

---

5 rede dielétrica ou subterrânea em fibra óptica, constituída por cabos que, em conjunção com equipamentos terminais adequados, permitem a disponibilização de canais de comunicação para serviços de transmissão de dados, voz e imagem.

O Wi-Fi é a redução do termo “*Wireless Fidelity*”. O Wi-Fi permite que os dispositivos se comuniquem sem o uso de fios. Para a transmissão dos dados, são utilizadas ondas de frequência de rádio, que atuam nas frequências de 2,4 GHz (mesma do micro-ondas) e 5 GHz.

O padrão utilizado na comunicação Wi-Fi é o IEEE 802.11 que promoveu a interação de serviços de redes por empresas diferentes. O padrão 802.11 tem suas variações de acordo com a faixa de frequência, velocidade e tamanho da chave de criptografia. (DANTAS, 2010).

1.3.4. *Power Over Ethernet* (PoE) e PoE +

A tecnologia *Power Over Ethernet* (PoE) permite que os equipamentos e dispositivos que se baseiam em IP (câmeras de vídeo IP, telefone IP, impressora, computador, por exemplo.) recebam simultaneamente a alimentação de energia elétrica e dados, partilhando a mesma infraestrutura de internet existente, reduzindo assim, os custos com a instalação separada. (RAMOS, 2013).

O PoE é uma funcionalidade de rede definida pelas normas do Instituto de Engenheiros Eletricistas **e** Eletrônicos (IEEE) 802.3af e 802.3at. Os dispositivos compatíveis com PoE podem ser equipamentos de fornecimento de energia *Power Sourcing Equipment* (PSE), dispositivos ligados *Powered Device* (PD) ou, por vezes, ambos. O dispositivo que transmite energia é um PSE, enquanto o dispositivo que recebe energia é um PD. A maioria dos PSE são switches de rede ou injetores de PoE destinados a utilização com switches não PoE. Os exemplos comuns de PD incluem telefones VoIP, pontos de acesso sem fios e câmaras IP. (RAMOS,2013).

Os equipamentos e dispositivos mais avançados baseados nesta tecnologia requerem maior valor de potência, e para isso criou-se uma norma, a norma IEEE 802.3at, conhecida como PoE+. A principal diferença entre o 802.3af (PoE) e o 802.3at (PoE+) é que os PSE com PoE+ podem fornecer quase o dobro da energia através de um único cabo de Ethernet. Os PSE com PoE+ podem fornecer energia a PD com PoE e PoE+, mas os PSE com PoE só podem fornecer energia a PD com PoE. Os PD com PoE+ exigem mais energia do que os PSE com PoE conseguem fornecer. (RAMOS,2013).

As informações contidas neste capítulo são essenciais para o conhecimento de tráfego de dados em uma rede e entre dispositivos, e irão auxiliar no entendimento de

como funciona um sistema de videomonitoramento que abordamos no capítulo seguinte.

2. VIDEOMONITORAMENTO

Na década de 30 iniciaram os primeiros testes com a televisão, e até a década de 70 ainda eram monocromáticas, tinham custo elevado e sem tecnologias consideráveis. Na década de 80 surgiram as câmeras coloridas a custo mais acessíveis para pequenas empresas. Nesse mesmo período surgiu a tecnologia *Video Home System* (VHS), possibilitando a gravação de imagens e com valor abaixo de 1000 libras esterlinas. (CIESZYNSKI,2004).

A princípio, o sistema de videomonitoramento necessitava apenas de câmeras, cabos e monitores de vídeo, porém, houve uma evolução para uma complexa configuração de equipamentos eletrônicos entrelaçados com computadores e tecnologias de telecomunicação. (HARWOOD, 2008).

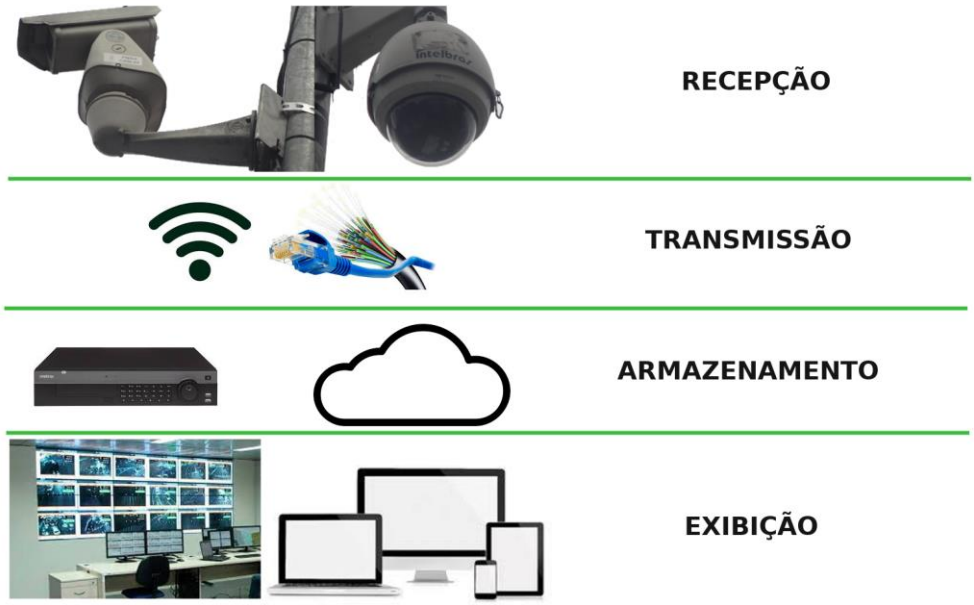
2.1. Circuito Fechado de Televisão (CFTV)

O Circuito Fechado de Televisão (CFTV) conhecido também como *Closed Circuit TeleVision (CCTV)*, o sistema de circuito fechado de televisão distribui sinais originados de câmeras instaladas em pontos determinados, até um local específico onde essas imagens serão supervisionadas e monitoradas. O funcionamento do CFTV pode ser dividido em 4 partes, conforme descrito a seguir e demonstrado na Figura 4:

- Equipamentos de recepção
- Meios de transmissão
- Meios de armazenamento
- Meios de exibição

Como equipamentos de recepção/captação podemos mencionar as câmeras. E como meios de transmissão podemos citar os cabos, fibras, Wi-Fi. Conforme descrito em capítulo anterior, os meios de armazenamentos são onde as imagens ficam gravadas, e detalharemos mais adiante, os meios de exibição são qualquer dispositivo com tela e acesso à internet como: celulares, tablets, PCs ou ainda um centro de monitoramento.

Figura 4: Componentes básicos de CFTV



Fonte: Autoria Nossa.

2.2. Tipos de Câmeras

As câmeras são classificadas de acordo com a tecnologia utilizada. Temos dois tipos de câmeras: as câmeras analógicas e a câmeras IP. (CIESZYNSKI, 2004).

As câmeras analógicas normalmente são conectadas por um cabo coaxial até um monitor que possibilite visualização das imagens geradas, e podem enviar simultaneamente as imagens geradas para os dispositivos de armazenamento, como por exemplo o *Digital Video Recorder* (DVR) e o *Network Video Recorder* (NVR). (CIESZYNSKI, 2004).

Já as câmeras IP não exigem a obrigatoriedade de uso de DVR ou NVR, pois contém um sistema operacional próprio que pode ser acessado diretamente por um navegador *web*, reduzindo o papel do NVR no sistema IP de realizar a gravação das imagens fornecidas pela câmera. (INTELBRAS, 2020).

A Figura 5 exemplifica a câmera panorâmica e câmera domo.

Figura 5: Câmera Panorâmica e Domo

Fonte: Autoria Nossa.

2.3. Video Management System (VMS)

O *Video Management System* (VMS) ou sistema de gerenciamento de vídeo é a referência mais comum dada a computadores, *hardware* e *software* usados nos sistemas de vídeo IP digital. O operador de um VMS é o controlador e gerente de vários sinais digitais, alarmes e controles *Pan-Tilt-Zoom* (PTZ) ou *speed dome*[6] .O VMS é uma réplica digital moderna de comutadores matriciais analógicos, que trata da gravação, visualização ao vivo e reprodução de fluxos de câmeras, sejam as câmeras analógicas convertidas em fluxos digitais ou digitais puros vindo diretamente de câmeras IP. (DAMJANOVSKI, 2014).

Toda a comunicação em um sistema VMS passa por cabos de rede de par trancado UTP ou redes sem fio. O principal componente de controle de *hardware* em um sistema VMS são computadores, na maioria das vezes executando o sistema operacional Windows e um aplicativo VMS. O *software* VMS é um aplicativo dedicado e instalado na parte superior do sistema operacional, que é capaz de selecionar câmeras, decodificar fluxos de vídeo e reprodução do hardware de gravação. (DAMJANOVSKI, 2014).

O hardware de gravação geralmente é um gravador de vídeo digital DVR ou NVR. Os DVRs e NVRs são tratados como dispositivos de gravação autossuficientes, e, como tal, eles raramente são executados no sistema operacional Windows, mas

6 câmera com zoom panorâmico e inclinação. É uma câmera capaz de controlar remotamente a direção e o zoom.

sim em Linux, que provou ser um sistema operacional mais estável. (DAMJANOVSKI, 2014)

2.4. Digital Video Recorder (DVR)

Um DVR é basicamente um computador que foi projetado para executar uma função, que é receber sinais de entrada de vídeo analógico e digital, digitalizar os sinais analógicos, comprimir todos os sinais conforme necessário e gravar esses sinais em um disco rígido. O gabinete do DVR pode ser de um design personalizado, ou pode ser uma torre padrão de computador, porém utiliza tecnologia de ponta para PC, incluindo um processador de alta velocidade, um disco rígido de grande capacidade, uma grande quantidade de *Random Access Memory* (RAM) e um sistema operacional. (CIESZYNSKI, 2004).

No início dos anos 90, a tecnologia do sistema de computadores ainda era muito limitada no que tange a capacidade de gravação, taxa de atualização de quadros e qualidade das imagens porém, à medida que a velocidade do processador e a capacidade de memória foram aumentando, o tamanho e a confiabilidade do disco rígido melhoraram e as técnicas de compressão foram evoluindo; observamos também uma melhoria constante no desempenho dos DVRs. Essa melhoria tende a ser constante, uma vez que a tecnologia continua elevando o seu grau de desempenho, bem como as técnicas de compressão. (CIESZYNSKI, 2004).

Mas o que torna um DVR melhor que outro? Diversos são os itens que contribuem para essa comparação, tais como: velocidade e tipo do processador, capacidade de RAM e do disco rígido, além do sistema operacional que pode influenciar na velocidade da máquina. Contudo, o que devemos considerar com maior grau de importância é a qualidade do disco rígido que deve ser usado para gravar as informações de vídeo digital. (CIESZYNSKI, 2004).

Um dos maiores problemas apresentados em DVRs é falha no disco rígido. Uma vez que normalmente funcionando 24hs, podendo levar ao desgaste do equipamento. (CIESZYNSKI, 2004).

Esses equipamentos devem ser de alta qualidade e devem possuir classe de servidor projetados para operação continua. A interface do usuário para um DVR varia consideravelmente. Vários fabricantes optaram por utilizar botões semelhantes ao de um equipamento VHS, pois consideram ser de mais fácil manuseio para os usuários

que não possuem uma habilidade mais técnica, uma vez que o DVR baseado em uma máquina adaptada, a interface do usuário tende a ser pelo monitor, e a operacionalização é feita com o mouse e o aplicativo de *software*. No entanto, deve-se tomar cuidado ao optar por usar DVRs que são baseados em computadores padrão, que foram adaptados pela instalação de uma placa de captura de vídeo e *software* de aplicação adequado. Essas máquinas devem incorporar uma unidade de disco rígido de alta qualidade para que funcionem de maneira confiável por um longo período, e devem ser testados antes de qualquer tomada de decisão (CIESZYNSKI, 2004).

2.5. Network Video Recorder (NVR)

Um NVR é usado para gerenciar e gravar imagens das câmeras IP, e não possui suporte às câmeras analógicas. Mesmo que seja possível acessar diretamente as imagens das câmeras IP, dispensando uso de um equipamento central, o uso do NVR se faz necessário ao utilizar várias câmeras e adiciona alguns benefícios e vantagens. A grande diferença da arquitetura analógica é que cada câmera é conectada por cabo coaxial diretamente ao DVR, enquanto que na arquitetura digital com dispositivos IP, o NVR e as câmeras são conectados na rede através de cabos de rede de par trançado UTP, fazendo com que o NVR consiga identificar na mesma rede as câmeras IP, fazer a gravação e gerenciar as imagens em um único ponto. (CIESZYNSKI, 2004).

Para a gravação e gerenciamento das imagens também é utilizado o *Hybrid Video Recorder* (HVR), conhecido como sistema híbrido. Ele gerencia e grava imagens tanto de câmeras analógicas, quanto de câmeras IP, e possui as mesmas funcionalidades mencionadas anteriormente. (CIESZYNSKI, 2004).

2.6. Codificadores/Decodificadores de Vídeos (CODECs)

Sem compressão de vídeo, os DVRs não seriam viáveis, pois os tamanhos de arquivos de imagens descompactadas ultrapassam a sua capacidade, e até as unidades de discos rígidos cujas capacidades são medidas em *terabytes,* ainda assim forneceriam registros limitados gravação, principalmente no que diz respeito ao limite de tempo. (CIESZYNSKI, 2004).

Se de um lado há o desejo de comprimir os sinais de vídeo para extrair o tempo máximo de gravação do DVR, por outro lado, a compressão excessiva resulta em perdas irrecuperáveis na informação da imagem, ocasionando a baixa qualidade na reprodução. O ideal é aplicar níveis de compressão suficientes para que haja uma alta capacidade de gravação, mas sem perder a qualidade ao extrair imagens de alta resolução da máquina. (CIESZYNSKI, 2004).

Muitas vezes esse procedimento torna-se inviável, pois é mais dispendioso, uma vez que irá requerer um maior número de DVRs, principalmente em sistemas com um número elevado de câmeras, além de exigirem um longo período de arquivamento. Por longos anos, foram utilizados dois métodos de compressão empregados nos DVRs de CFTV: MPEG-2 e Wavelet (agora JPEG 2000). Contudo, desde a implementação do MPEG-4, muitas máquinas estão migrando para esse formato de compactação, pois oferece melhor qualidade de imagem que o MPEG-2. (CIESZYNSKI, 2004).

2.7. Firmware

A maioria dos dispositivos embarcados necessitam de algum *software* personalizado para funcionar. Esses softwares são denominados *firmware* e podem ser atualizados e carregados quando necessário.

Normalmente, as atualizações de *firmware* são disponibilizadas nos sites dos fabricantes ou apresentam atualização automáticas quando solicitadas. A análise interna de um arquivo de firmware pode revelar muitas informações sobre o dispositivo, como: senhas padrão, portas administrativas e interfaces de depuração. (HACKERS EXPOSTOS 7, 2014)

Conforme cada vez mais sistemas são utilizados, mais mecanismos de segurança são necessários, e nesse contexto surge a segurança da informação que será apresentada no próximo capítulo.

3. SEGURANÇA DA INFORMAÇÃO

Conforme ABNT NBR (Associação Brasileira de Normas Técnicas, 2005), a informação é considerada um ativo de muita importância para um negócio, e por isso deve ter a sua proteção de forma adequada.

Já a ABNT NBR ISO/IEC 27001(Associação Brasileira de Normas Técnicas ISO/IEC 27001, 2013), diz que os ativos mais relevantes devem ser identificados e devidamente inventariados, além de classificá-los como ativos de informação, por exemplo: os bancos de dados de softwares: como as aplicações; físicos: como os computadores, e de serviços: como os serviços de comunicação.

Para Mandarini (2004), a Segurança da Informação visa a proteção contra ameaças com o objetivo de diminuir perdas, aumentar o retorno dos investimentos feitos e assegurar a continuidade do negócio da organização.

Segundo o Tribunal de Contas da União (TCU, 2003), a Segurança da Informação tem o intuito de proteger os seus mencionados pilares: confidencialidade, integridade, disponibilidade e a autenticidade.

A informação deve ser protegida em todo o seu ciclo de vida que, o que implica desde o momento do manuseio, do armazenamento, do transporte e do seu descarte. (ISO/IEC 27001, 2013).

3.1. Vulnerabilidades

Segundo Beal (2008), vulnerabilidade é uma debilidade que pode ser usada para realizar um ataque. As vulnerabilidades são brechas que usuários mal-intencionados utilizam para acessar os conteúdos de um sistema, ocorre na maioria das vezes em sistemas desatualizados.

A ABNT NBR ISO/IEC 27002(Associação Brasileira de Normas Técnicas ISO/IEC 27004, 2005) define a vulnerabilidade como uma fragilidade de um ativo que pode ser explorada por uma ou mais ameaças, permitindo a ocorrência de incidentes na segurança da informação.

Ameaça é a perspectiva de que ocorra um acontecimento de forma acidental ou até proposital, por um agente, que venha a afetar um ambiente, ou um sistema ou um ativo de informação. Considera que impacto é o efeito ou a consequência que um ataque ou incidente pode vir a trazer para a organização. (BEAL, 2008).

Qualquer sistema computacional sem os devidos controles de segurança, ou se estiverem desatualizados, ou com configurações indevidas, estão suscetíveis a potenciais problemas com a segurança de seus dados. (ABNT NBR ISO/IEC 27002, 2005).

3.2. Malware

Malwares são programas ou softwares ou código maliciosos que têm o objetivo de acessar dispositivos sem autorização, violando a privacidade do dono, de forma que venha a comprometer a segurança dos dados e das informações desses dispositivos.

A palavra *Malware* é a abreviação de "*malicious software*" que traduzindo fica "*software* malicioso".

Os tipos de *malwares* e ataques abordados são: *spams*, *trojan*, vírus, *phishing, worm* (Steding-Jessen 2008) e DDoS (Binsalleeh et al. 2009).

Conforme definido pela Cert (2019), descrevemos a seguir os tipos de *malwares*:

- *Spams:* é o nome utilizado para referenciar *e-mails* recebidos sem terem sido solicitados, normalmente enviados para diversas pessoas. Muitos spams são e-mails contendo propagandas de produtos ou serviços, mas também é uma forma de propagação de códigos maliciosos.
- *Trojan:* O Cavalo de Tróia, também conhecido como trojan, é um programa criado para executar funções na sua maioria maliciosas, sendo algumas sem o consentimento do usuário.

Esse tipo de programa precisa ser executado para serem instalados efetivamente no computador. Alguns vem acompanhados junto a coisas simples obtidas pela internet, como por exemplo jogos, protetor de tela, fotos etc.

Os programas *antimalwares* têm uma coletânea de trojans categorizados como os seguintes exemplos:

a. *Trojan Downloader*: que é obtido pela internet e faz a instalação de códigos maliciosos.

b. *Trojan Backdoor*: que possibilita que seja realizado o acesso de forma remota pelo atacante.

c. *Trojan* Destrutivo: que pode apagar e alterar arquivos e pastas, formatar o disco rígido e deixar o computador em estado não-operacional.

- Vírus: O vírus de computador é um programa malicioso que infecta o dispositivo e se espalha para arquivos e/ou outros programas, dependendo para isso da execução do programa ou arquivo que o hospeda.

Um computador infectado pode apresentar as seguintes características, segundo a *Avast*:

a. Conexão de internet lenta ou inexistente;

b. Desativação do software de Antivírus e do *firewall*;

c. Execução de atividades e ações sem a solicitação ou o consentimento do dono.

- *Phishing*: é um programa malicioso usado por fraudadores com o objetivo de efetuar o roubo de senhas. Um exemplo disso são as falsas páginas de *Home Banking*. Se assemelham muito com as páginas originais, mas ao digitar os dados de agência conta e senha, o usuário tem seus dados repassados ao criminoso.
- *Worm*: é um programa que tem a capacidade de se espalhar de forma automática pelas redes, através do envio de sua própria cópia de computador a computador.

Ao contrário dos vírus, o *Worm* se propaga através execução de sua cópia e não pela simples inserção dela.

Na sua propagação e contaminação, o *Worm* identifica os computadores que serão alvos, faz o envio de cópias de si para esses alvos, ativa as cópias através de sua execução e reinicia o ciclo.

- *DDoS:* é um ataque realizado com a finalidade de tirar uma operação ou um serviço do ar, ou seja, deixando-o indisponível através de muitas solicitações direcionadas a este, ou pela projeção de um tráfego muito grande de dados para a rede do alvo.

Às vezes, o computador pode ser utilizado nesse ataque sem conhecimento de seu dono por estar contaminado e fazer parte de uma rede de *bots*.

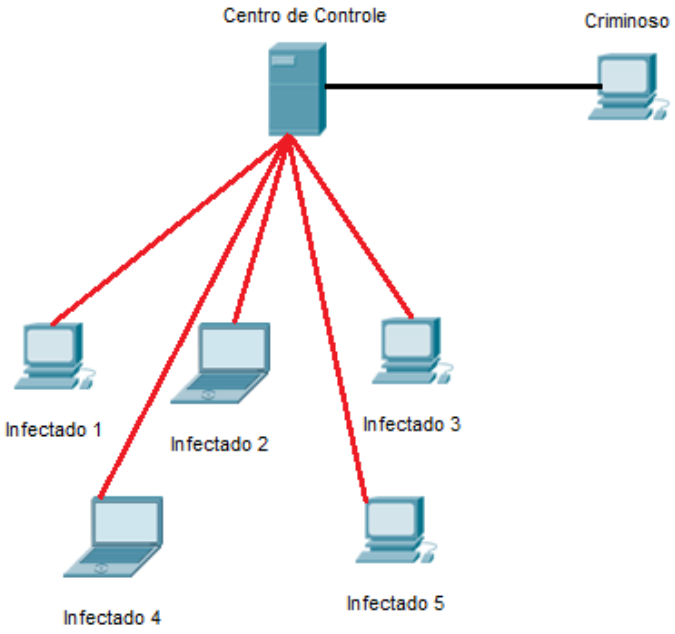
3.3. Botnet

Botnet é uma rede de computadores infectados por algum tipo de vírus ou malware, e é por diversas vezes utilizados para atividades criminosas. A origem da palavra vem da junção da palavra "*bot",* que significa robô, e "*net"* a contração da palavra *network*, que significa rede. (CERT, 2012).

Para Sacchetin (2008), *Botnet* é um tipo de rede com muitos computadores que tenham sido contaminados e estão sendo comandados por um controlador central (o criador do malware que possui o controle do dispositivo), tornando os computadores afetados como zumbis. Conforme a Figura 6, são definidos os seguintes componentes:

- Infectados: Dispositivos (*bots*) que foram infectados e controlados pelo malware;
- Criminoso: Controlador de toda a rede de bots;
- Centro de controle: Utilizado como ferramenta de envio de comandos para os dispositivos afetados.

Figura 6: Diagrama da Botnet



Fonte: Autoria Nossa.

Segundo a ENISA (2011), as *Botnets* normalmente são para crimes cibernéticos como o roubo de informações e dados pessoais como os de cartões de créditos.

Além disso, outros objetivos mencionados por SACCHETIN (2008), seriam:

- Efetuar coletas de informações
- Orquestrar ataques de negação de serviço (*DDoS*),
- Enviar spam e propagar vírus.

De acordo com a ENISA (2011), *botnets* costumam ter dois tipos diferentes de organização: Centralizada ou descentralizada. O modelo centralizado segue como base a arquitetura cliente-servidor e é o mais comum de se encontrar, nesse modelo os *bots* dependem de se comunicar com o centro de controle para executar as ações. Já o modelo descentralizado utiliza a arquitetura de rede *peer-to-peer* (P2P), este não possui um ponto central para controlar a *botnet*.

Os computadores infectados por *Botnet* podem apresentar algumas falhas, dentre elas estão: reiniciar sem o usuário ter comandado, lentidão, mensagens de erros etc.

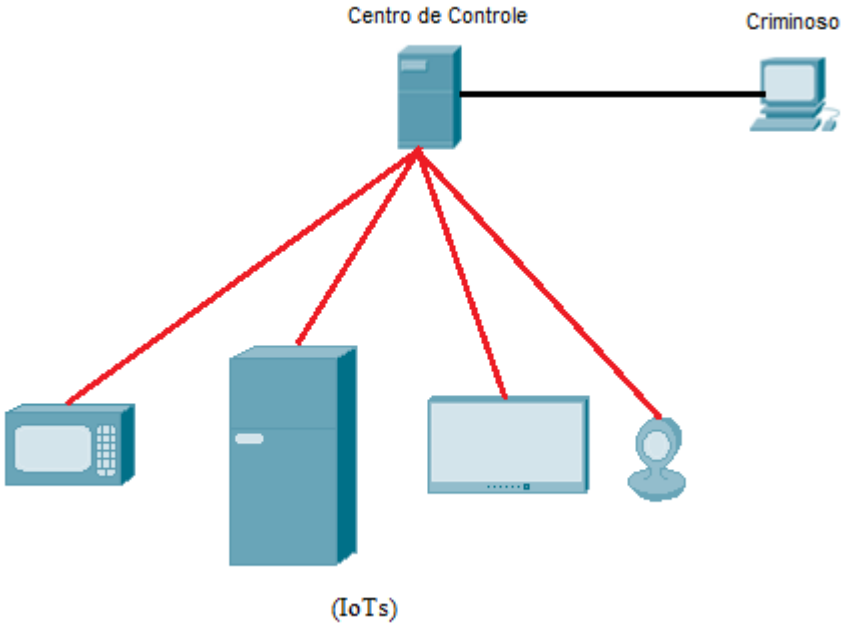
3.4. Mirai

O *Mirai* é o nome dado a um tipo de malware que foi desenvolvido para criar botnets e com o objetivo de executar ataques *DDoS*, e atinge principalmente dispositivos de *Internet Of things* (IoT).

O objetivo, segundo a ENISA (2011), é de alistar os dispositivos IoT em uma grande rede de *bots* e praticar ataques cibernéticos.

O criminoso pode tomar controle total dos dispositivos e acessá-los de forma remota, conforme mostra a Figura 7.

Figura 7: Diagrama do Mirai



Fonte: Autoria Nossa.

As vulnerabilidades são cada vez mais exploradas o que pode levar as organizações a terem grandes perdas. No capítulo seguinte analisamos as vulnerabilidades contidas nos sistemas de videomonitoramento e construímos um *check list* com o intuito de mitigar os riscos na implantação de novos sistemas de segurança.

4. VULNERABILIDADES EM CFTV

Quando falamos em videomonitoramento priorizamos a segurança física das pessoas como proporcionar segurança e conforto nos ambientes, controle de acesso de pessoas autorizadas a determinado ambiente, na segurança patrimonial etc.; mas o sistema de videomonitoramento vai muito além desses itens. Ao implantar esse tipo de sistema, será que são considerados os seguintes itens: vulnerabilidades dos equipamentos utilizados, onde as informações serão armazenadas, quem terá acessos a essas informações/imagens, segurança do local onde as informações são guardadas etc. Baseado nesses itens elaboramos uma pesquisa um pouco mais detalhada dessas possíveis falhas no sistema de videomonitoramento.

Existem diversos fatores que estão relacionados diretamente com as vulnerabilidades, como por exemplo: fragilidades nos equipamentos, nos processos, nas políticas e nos recursos humanos. (SILVA, 2018).

Segundo a CERT (2017)**,** quando uma vulnerabilidade é explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Para se construir um sistema de monitoramento, existem diferentes tecnologias disponíveis e eficientes. O circuito fechado de televisão CFTV, que consiste num conjunto de câmeras que captam as imagens e as transmitem até um sistema de televisão. Os sistemas atuais podem transmitir as imagens das câmeras através de cabos de rede *Ethernet* ou através de rede *Wi Fi* por meio de dispositivos *Wireless*, podendo gravar as imagens capturadas pelas câmeras em um computador local ou até mesmo na nuvem, proporcionando um maior conforto, comodidade e flexibilidade. Uma rede sem fio transmite dados utilizando sinais de rádio frequência e infravermelho que permitem mobilidade contínua através de sua área de abrangência (SILVA, 2018).

Com base nos itens mencionados analisamos as principais vulnerabilidades em cada um deles, que devem servir como um direcionamento para a elaboração do *check list* (objetivo do nosso trabalho) para que possa ser utilizado em futuras instalações em sistemas de videomonitoramento em vias públicas.

4.1. Vulnerabilidades em Câmera de videomonitoramento

As câmeras de CFTV são consideradas vulneráveis, pois são configuradas com logins e aceitam conexões de quaisquer pessoas conectadas à internet. As câmeras de CFTV não são apenas câmeras, são computadores, executam softwares e estão conectados à Internet. E muitos deles são mal protegidos, com senhas padrão, o que facilita o acesso dos crackers, que podem fazer um ataque de dicionário de força bruta, por exemplo, contra os dispositivos de CFTV para obter acesso, trabalhando com uma lista de senhas prováveis. (CLULEY, 2015).

Tais vulnerabilidades podem comprometer o sistema de videomonitoramento, bem como colocar em risco a vida de diversas pessoas, causando a exposição de informações pessoais.

Segundo Ribeiro (2015, p.20):

> “A privacidade é considerada uma questão crítica, uma vez que as informações armazenadas e trafegadas expõem os comportamentos e hábitos dos consumidores. Determinadas atividades podem ser identificadas a partir de padrões de consumo elétrico, identificar se os moradores estão em casa, trabalhando ou viajando, assistindo televisão ou se possuem cerca elétrica. A demanda por soluções para a segurança e privacidade torna-se cada vez mais evidente, não bastando utilizar soluções de criptografia, controle de acesso e autenticação, mas sim uma perspectiva arquitetural voltada para a segurança e privacidade.”

Certas falhas permitem que invasores acessem o áudio e vídeo das câmeras, desativem os dispositivos, executem código malicioso e muitas outras coisas remotamente.

É importante ressaltar que esses ataques são possíveis se os invasores conhecerem o modelo das câmeras. Porém, podem descobrir facilmente por meio de ataques simples de força bruta.

Alterar a senha padrão das câmeras e de DVRs não garantem proteção total. As câmeras de segurança possuem um sistema operacional interno que podem ter vulnerabilidades conhecidas pelos crackers que irão explorá-las para ter acesso ao

sistema. Além disso, devido ao baixo custo desse sistema, em consequência a demanda de clientes, muitos fabricantes não se preocupam com os detalhes das vulnerabilidades dos produtos que comercializam, e nunca são atualizados. Uma vez instalados e conectados à internet, já estão em risco. (NETDEEP, 2019).

As pessoas não se interessam em aprender como funciona a configuração de acesso remoto e não querem aprender sobre redes IPs e segurança, pois são orientadas por técnicos a utilizarem uma rede *Demilitarized Zone*[7] *(*DMZ), o que é uma brecha para aumentar a invasão de câmeras de segurança e DVRs, comprometendo também a rede interna. Para ter acesso ao sistema operacional desses equipamentos basta que acessem os sites dos fabricantes e baixem o firmware. Feito isso começam a explorar as falhas de segurança e a espalharem a notícia. (NETDEEP, 2019).

4.2. Vulnerabilidades em protocolos de transmissão

Outra vulnerabilidade encontrada é a transmissão de vídeo não criptografada. Um terreno fértil para ataques de interceptação *Man in the Middle* (MITM) e permitindo que intrusos espionem as imagens de vídeo das vítimas". um criminoso intercepta o tráfego de rede entre o aplicativo de monitoramento e a nuvem ou entre a nuvem e a câmera, pode usar os dados transmitidos da conexão TCP na porta do servidor (nuvem) 2048 para ver as solicitações HTTP dos pacotes de áudio e vídeo. (NETDEEP, 2019).

4.3. Vulnerabilidades em meios de armazenamento

As informações são armazenadas em suportes físicos (disco rígido, CD, DVD) ou magnéticos (Cartão de memória, *Pen drive*, fitas magnéticas etc.).

Suas utilizações inadequadas, como por exemplo, prazo de validade, defeito de fabricação, uso incorreto, podem ocasionar uma vulnerabilidade, afetando a integridade, a disponibilidade e a confidencialidade das informações. (NASCIMENTO, 2013).

As ameaças de segurança na nuvem são semelhantes aos riscos de armazenar dados em qualquer outro lugar. Os dados na nuvem estão armazenados em um data

---

7 zona desmilitarizada, também muito conhecida como rede de perímetro, é uma área física, ou em alguns casos lógica, que expõe serviços de uma organização a uma rede não confiável, a Internet.

center, e mesmo assim, podem ser acessados por crackers por meio de muitos métodos como: *phishing* de e-mail, senhas fracas e falta de autenticação multifator.

As principais ameaças à segurança da nuvem que merecem destaque são: a ameaça interna, o risco de perda de dados e a devida monitoração. (MINDSEC, 2018)

4.4. Vulnerabilidades Físicas

As vulnerabilidades físicas estão relacionadas ao ambiente onde as informações são processadas, como por exemplo, pessoas não identificadas ao local, processo de migração de servidores onde um funcionário falha em seguir os protocolos de segurança durante o procedimento, instalações inadequadas, ausência de recursos para combate a incêndio; disposição desordenada dos cabos de energia e de rede; portas destrancadas; sistema deficiente de combate a incêndio; edifícios mal projetados e mal construídos, acesso desprotegido aos servidores que armazenam as informações coletadas pelos dispositivos, etc. (SILVA, 2018).

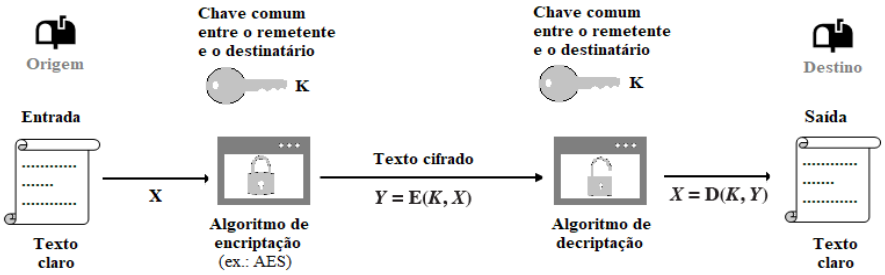
4.5. Criptografia

Segundo Denning (1982), os mecanismos de criptografia foram criados para transmitirem informações com mensagens secretas a fim de garantir a confidencialidade ou autenticidade da informação. Uma cifra é o método de escrita em que em um texto simples (sem criptografia) é transformado em texto cifrado ou criptografado. O processo inverso é chamado de decifrar.

Os principais algoritmos de criptográfica são simétricas e assimétricas.

Segundo Cavalcante (2004), a criptografia simétrica consiste em cifrar e decifrar um texto utilizando única chave privada de codificação, conforme podemos ver na Figura 8.

Figura 8: Diagrama de Criptografia Simétrica



Fonte: Autoria Nossa

Já a criptografia assimétrica, faz o uso de duas chaves sendo uma pública para cifrar a mensagem, e uma privada para decifrá-la. Um exemplo é o algoritmo *RSA* que utiliza expressão com exponenciais. (CAVALCANTE, 2004).

4.6. Mitigação das Vulnerabilidades

Se faz necessário uma análise de riscos em que sejam identificadas as vulnerabilidades, as ameaças, os agentes que podem explorá-las e a probabilidade de ocorrer cada uma das vulnerabilidades. Após realizada a análise de risco, será necessário estabelecer ações preventivas, reativas e corretivas com o intuito de reduzir os riscos. (HINTZBERGEN, SMULDERS, BAARS, 2018).

Com a finalidade de elaborar o *check list,* foi realizado o mapeamento de riscos e vulnerabilidades em sistemas de CFTV, conforme quadro 1. Nele, foram elencados os ativos e/ou componentes, suas respectivas vulnerabilidades, as ameaças à segurança, as medidas de mitigação e quais os benefícios dessas medidas.

Quadro 1 Análise de Vulnerabilidades

Ativos/ Componentes	Vulnerabilidades	Ameaças	Mitigações	Objetivos/ Benefícios
Câmeras	Firmware desatualizado	Exploração das vulnerabilidades ainda não corrigidas pelo fabricante/ desenvolvedor do software para ataques e/ou acessos indevidos.	Assim que lançada a nova atualização do software pelo fabricante, verificar as correções feitas e realizá-la. Comprar de fabricantes conhecidos, pois estes tentam manter a reputação e mantém atualizações por mais tempo	Garantir maior índice de segurança. Atualizar os softwares para a sua correta funcionalidade e/ou agilidade. Corrigir as novas vulnerabilidades identificadas.
Câmeras	Senha padrão	Terceiros tendo acesso facilitado por conhecerem senha e usuário padrão do fabricante.	Fazer troca da senha padrão por uma senha própria.	Dificultar o acesso não autorizado.
Rede	Uso de protocolos inseguros e/ou sem criptografia	Interceptação de dados e visualização de informações sigilosas por terceiros.	Usar criptografia de dados.	Garantir a confidencialidade.
Rede - WIFI	Criptografia fraca	Facilita a invasão da rede por terceiros.	Dar preferência por uso de algoritmos atualizados.	Evitar que usuários não autorizados se conectem na rede
Armazenamento	Falhas em disco	Perda de dados	Utilização de backup de dados, gravação remota	Garantir disponibilidade dos dados

DVR/NVR	Local inapropriado	Possibilidade de roubo do aparelho	Armazenar o aparelho em local seguro onde poucas pessoas possuem acesso.	Garantir disponibilidade dos dados
DVR/NVR	Firmware desatualizado	Exploração das vulnerabilidades ainda não corrigidas pelo fabricante/ desenvolvedor do software para ataques e/ou acessos indevidos.	Executar atualizações constantes do firmware, assim que lançado uma nova versão. Comprar de fabricantes conhecidos, pois estes tentam manter a reputação e mantém atualizações por mais tempo	Garantir maior índice de segurança; receber correções de sistema do software que visam a sua correta funcionalidade e/ou agilidade; receber a correção novas vulnerabilidades identificadas.

Fonte: Autoria Nossa.

4.7. Checklist

Com base em toda a pesquisa realizada e conforme o mapeamento de vulnerabilidades, foi elaborado o modelo de *checklist* (Apêndice A) no qual será possível analisar e apontar se todas as medidas de segurança foram ou não aderidas no sistema de videomonitoramento.

Caso alguma das medidas de segurança mencionadas no *check list* não tenham sido seguidas, será necessária a devida correção antes da implantação do sistema.

5. CONSIDERAÇÕES FINAIS

O modelo de *Check List* elaborado no presente trabalho visa a sua utilização em novas implantações de sistemas de videomonitoramento em centros urbanos.

Os profissionais de Segurança da Informação, além de garantir que os pilares da segurança não sejam violados, de certa forma, também são corresponsáveis por zelarem pela segurança das pessoas.

Após a visita em um centro de monitoramento de vias urbanas, foram verificadas algumas fragilidades que nem sempre são levadas em consideração por aqueles que tem acesso ao local, bem como o devido cuidado com o armazenamento das imagens.

É de responsabilidade dos órgãos competentes garantir a segurança pública dos cidadãos, porém, é de responsabilidade de profissionais de segurança da informação garantir que as informações e dados desses cidadãos não sejam expostos e acabem sendo utilizados por pessoas má intencionadas.

Durante a pesquisa, bairros foram percorridos, identificando onde essas câmeras estão instaladas e para onde estão apontadas. Foram levantados alguns questionamentos quanto as falhas apresentadas nesse sistema, e por isso, decidiu-se explorar algumas delas, bem como propor a correção para mitigar os riscos.

Além disso, houve a preocupação de informar àqueles que possam vir a ler esse trabalho, como funciona o serviço de videomonitoramento, o tráfego das informações, uma vez que esse processo está cada vez mais presente em nosso dia a dia.

Será de suma importância seguir os passos elencados no *Check List* para a implantação de novos sistemas de videomonitoramento ou para corrigir os sistemas que já estão em funcionamento, pois, dessa forma garante-se a redução de riscos no que diz respeito a invasão de um sistema de segurança, bem como a guarda correta das informações evitando expor a privacidade das pessoas.

REFERÊNCIAS

ABNT. NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro. ABNT, 2006.

ALVES, Paulo. **Falha em sistema de câmera de segurança vaza dados de 2,4 milhões de usuários.** Disponível em: https://www.techtudo.com.br/noticias/2020/01/falha-em-sistema-de-camera-de-seguranca-vaza-dados-de-24-milhoes-de-usuarios.ghtml. Acesso em: 19/06/2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – **ABNT. NBR ISO/IEC 27002**: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2007.

AVAST. **Botnet.** Disponível em: <https://www.avast.com/pt-br/c-botnet>. Acesso em 27/03/2020.

AVAST. **Vírus de Computador.** Disponível em: <https://www.avast.com/pt-br/c-computer-virus>. Acesso em 01/04/2020.

BARRETT, Diane; KING, Todd. **Redes de computadores**. Rio de Janeiro: LTC, 2010.

BEAL, ADRIANA. Segurança da informação. Princípios e melhores práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Editora Atlas, 2008.

CAPUTO, C. Anthony. **Digital Video Surveillance and Security**. Oxford: Elsevier, 2014.

CARTLIDGE, ALISON; LILLYCROP, MARK. **The IT Infrastructure Library: An Introductory Overview of ITIL - Version 3**. Wokingham, United Kingdom: IT Service Management Forum, 2007.

CAVALCANTE, A.L.B. **Matemática II**- Notas de Aula. Brasília: Editora UPIS, 2004.
CIESZYNSKI, Joe. **Closed Circuit Television**. Oxford: Elsevier, 2004.

CLULEY, G. Hacked shopping mall cctv cameras are launching ddos attacks. Tripwire, 2015. Disponível em: <https://www.tripwire.com/state-of-security/security-data-protection/hacked-shopping-mall-cctv-cameras-are-launching-ddos-attacks/>. Acesso em: 18/06/2020.

Comitê Gestor da Internet no Brasil - **Cartilha de Segurança para Internet**, versão 4.0 / CERT.br – São Paulo, 2012.

COMPUTERWORLD, from IDG. **Câmeras de vigilância apresentam vulnerabilidades graves de segurança**. Disponível em: <https://computerworld.com.br/2018/03/15/cameras-de-vigilancia-apresentam-vulnerabilidades-graves-de-seguranca/>. Acesso em: 19/06/2020.

DAMJANOVSKI, Vlado. **CCTV: Networking and Digital Technology**. Oxford: Elsevier, 2005.

DAMJANOVSKI, Vlado. **CCTV: Networking and Digital Technology** Butterworth-Heinemann 2014.

DANTAS, Mario. **Redes de comunicação e computadores:** abordagem quantitativa. Florianópolis: Visual Books, 2010.

DENNING, Dorothy E. **Cryptography and data security.** Addison-Wesley, 1982.

DIAS, Matheus Brum; GONÇALVES, Isabelle Ribeiro; SANTOS, Felipe de Abreu Marques dos. **Internent das coisas (IoT). Estudo de vulnerabilidades em Smart Home**. Disponível em: <https://drive.google.com/drive/folders/1wok6TiZXcrRevDWGGbzae_0uIJJ5ZTt1>. Acesso em: 18/06/2020.

DIRETORIA DE AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO DO TRIBUNAL DE CONTAS DA UNIÃO. **Boas Práticas em Segurança da Informação**. Brasília, 2003.

ENISA. **“Mirai” malware, attacks Home Routers**. Disponível em: <https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers>. Acesso em 24/03/2020.

ENISA. **Botnets**. Disponível em: <https://www.enisa.europa.eu/events/botnets>. Acesso em 24/03/2020.

ESET. **Vulnerabilidade em câmeras D-Link permite que atacantes possam espionar transmissões**. Disponível em: <https://www.welivesecurity.com/br/2019/05/03/vulnerabilidade-em-cameras-d-link-permite-que-atacantes-possam-espionar-transmissoes/>. Acesso em: 19/06/2020.

FONTES, E. L. G. **Praticando a Segurança da Informação**. 4. ed. Rio de Janeiro: Brasport, 2008.

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

HARWOOD, Emily. **Digital CCTV: A Security Professional’s Guide**. California: Elsevier, 2008.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 3. ed. aum. Rio de Janeiro: Brasport, 2018. 150 p. v. 1. ISBN 978-85-7452-867-0.

H. Schulzrinne, A. Rao, R. Lanphier, M. Westerlund, M. Stiemerling, Ed. **Real Time Streaming Protocol**. Disponivel em: <https://www.ietf.org/rfc/rfc2326.txt>.Acesso em: 29/10/2019.

IETF. **Real Time Streaming Protocol**. Disponível em: <https://www.ietf.org/rfc/rfc2326.txt>.Acesso em: 29/10/2019.

KRUEGLE, Herman. CCTV Surveillance: Video Practices and Technology. Oxford: Elsevier 2007.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet:** uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informação gerenciais**. 7. ed. São Paulo: Pearson, 2007.

MANDARINI, M. **Segurança Corporativa Estratégica**. São Paulo: Usina do Livro, 2004.

MAYA, Alcides. **O que são redes de computadores?** Disponível em: <https://alcidesmaya.edu.br/redes-de-computadores/o-que-sao-redes-de-computadores/>. Acesso em: 13/04/2020.

MINDSEC. Minuto da Segurança. **As 12 maiores ameaças à segurança na nuvem.** https://minutodaseguranca.blog.br/top-12-cloud-risk/. Acesso em: 20/06/2020.

NASCIMENTO, Nelson José do. **Ameaças e vulnerabilidades da informação. Como precaver!** Disponível em: https://www.portaleducacao.com.br/conteudo/artigos/pedagogia/ameacas-e-vulnerabilidades-da-informacao-como-precaver/48819. Acesso em: 20/06/2020.

NETGEAR, support. **O que é o PoE? (Power over Ethernet).** Disponível em: <https://kb.netgear.com/pt_PT/209/O-que-é-o-PoE-Power-over-Ethernet>. Acesso em: 22/03/2020.

PREFEITURA MUNICIPAL DE SANTO ANDRÉ. **Anuário de 2016 – Ano Base 2015**. <https:// https://www2.santoandre.sp.gov.br/index.php/dados-estatisticos >. Acesso em 29/10/2019.

RAMOS, Sergio Felipe Carvalho. **Power Over Ethernet: A Solução de Vanguarda nas Comunicações Baseadas em IP**. *Neutro à Terra*, (12). Disponível em:<https://doi.org/10.26537/neutroaterra.v0i12.388>. Acesso em: 22/02/2020.

REIS, Rodrigo. **Modelo TCP/IP – Definição, camadas e funcionamento.** Infotec News. Disponível em: <http://infotecnews.com.br/modelo-tcpip/>. Acesso em: 19/06/2020.

SACCHETIN, M. C. et al. **Botnet detection and analysis using honeynet**. International Journal of Forensic Computer Science, 2008.

SECRETARIA DE SEGURANÇA PÚBLICA DO ESTADO DE SÃO PAULO. **Divisão dos CONSEGs**. Disponível em: <http://www.ssp.sp.gov.br/CONSEG/Localiza/LocalizeConseg>. Acesso em: 29/10/2019.

SILVA, Augusto Moura Alves. **Segurança para câmeras IP**. Disponível em: <https://repositorio.ufu.br/bitstream/123456789/26148/3/Seguran%C3%A7aC%C3%A2merasIP.pdf>. Acesso em: 19/06/2020.

SILVA, Tiago Antônio da. O que são redes de computadores. Disponível em: <https://pt.slideshare.net/TiagoSilva12/o-que-so-redes-de-computadores>. Acesso em 13/04/2020.

REPORT, Security. **Câmeras inteligentes: falhas permitem acesso de hackers**. Disponível em: <https://www.securityreport.com.br/overview/cameras-inteligentes-falhas-permitem-acesso-de-hackers/#.XuzDU2hKg2w>. Acesso em: 19/06/2020.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TECNOLOCIA, Netdeep. **Segredos dos hackers que invadem câmeras de segurança e DVRs**. Disponível em: <https://www.netdeep.com.br/blog/segredos-dos-hackers-que-invadem-cameras-de-seguranca-e-dvrs/>. Acesso em: 19/06/2020.

APÊNDICE A

	ITENS PARA VERIFICAR	VERIFICADO	COMENTÁRIOS
Recepção	Alterar todas senhas padronizadas pelos fabricantes		
	Os firmwares estão atualizados com a última versão do fabricante?		
	Trocar porta padrão de acesso		
	Desabilitar o uso de DMZ		
Transmissão	Se wi-fi, qual protocolo de transmissão? É a versão mais recente?		
	Usa alguma proteção na transmissão de dados como VPN ou criptografia?		
	O sinal de vídeo precisa ser criptografado?		
Armazenamento	Alterar todas senhas padronizadas pelos fabricantes		
	Os firmwares estão atualizados com a última versão do fabricante?		
	Desabilitar o uso de DMZ		
	Além do DVR/NVR, existe outro local onde são armazenadas as imagens?		
	Se DVR/NVR o local instalado tem a devida segurança?		
Exibição	Alterar todas senhas padronizadas pelos fabricantes		
	Os firmwares estão atualizados com a última versão do fabricante?		
	Desabilitar o uso de DMZ		
	O software VMS está com a versão mais recente?		

Recepção	Câmeras
Transmissão	Cabos, fibra ótica, wi-fi
Armazenamento	DVR, NVR, Cloud
Exibição	PC, celular, tablet, software VMS

Responsável: _____

Verificado em: _____

APÊNDICE B

Trata-se de uma pesquisa parcial da região da cidade onde concentramos nosso objeto de estudo. Em apenas 10 bairros, registramos os locais onde há câmeras instaladas em áreas de passagem pública, como calçadas, por exemplo.

O objetivo foi levantar a quantidade de câmeras e para onde essas câmeras estavam sendo apontadas.

Nos resultados, os números relacionados as câmeras, foram levantados pelo grupo de forma manual, enquanto as extensões das vias foram medidas através do uso do *Java Open Street Map* (JOSM) e com o *plugin Measurements*.

Já as vias mapeadas da região pesquisada no *Open Street Map* e as relações, foram calculadas baseadas em alguns dados adquiridos do anuário de Santo André de 2016 ano base 2015 no site da prefeitura.

Legenda:

Nº = Número da casa
Q = Quantidade total de câmeras
B= Câmera do tipo bullet
D= Câmera do tipo domo,
O= Outros tipos de cameras (*webcam*, *speed dome* etc).