Facens

FACULDADE DE ENGENHARIA DE SOROCABA

PROJETO CONNOR

MONITORAMENTO DE REDES

RELATÓRIO DE MONITORAMENTO

Filipe Sousa
Lucca Campos
Otávio Marelli
Renato Júnior
Stephanie Braga

Orientadores: Andreia Leles
Luciano Freire

Sorocaba / SP
05 / 08 / 22

Autor	Revisão	Descrição
FSS, LPC, OMM, RNJ, SMB	00	Criação do documento base e adição de todo conteúdo.

Sumario

Lista de Figuras

1. INTRODUÇÃO

A implementação de uma rede segura em um ambiente corporativo, garante que camadas de segurança sejam adicionadas à rede, protegendo as conexões e informações e preservando a integridade desses dados, principalmente quando se trata de dados pessoais sensíveis. Para que a segurança seja implementada no ambiente, há normas que abordam os principais pontos e auxiliam na criação de métodos.

A norma ISO descreve as melhores práticas para as empresas e como benefício conseguem ter uma conscientização sobre os riscos que sua rede está correndo, controle das informações, criação de uma política de segurança, possibilidade de identificar e corrigir algum problema da rede, se torna um diferencial competitivo, organização de processos, redução de custos e prevenção de incidentes, além de estar em conformidade com a legislação.

De acordo com norma, o uso de softwares e ferramentas que façam o monitoramento da rede é importante para que possíveis gargalos, ataques ou incidentes que estejam acontecendo na rede sejam detectados a tempo. Para atender a norma, o uso de duas ferramentas de monitoramento, o Zabbix e o Grafana, foram utilizados durante o projeto de monitoramento do campus. Assim, os equipamentos do campus estão registrados e são monitorados através do Zabbix, que coleta as principais informações relacionadas a trafego de pacotes, disponibilidade e uso de CPU.

No Grafana, esses indicadores são utilizados para mostrar de forma gráfica os dados que estão sendo coletados e isso favorece o TI, que visualiza de forma rápida o que está acontecendo e em tempo real, facilitando uma ação adequada.

Além de realizar o monitoramento dos equipamentos que estão conectados na rede, a utilização de ferramentas para ter segurança em aplicações web e na rede é um complemento para a gestão dos riscos.

O OWASP é um dos principais guias para segurança em aplicações web e utilizado junto com as ferramentas de IAST, SAST e DAST, garante que todo o ciclo de desenvolvimento esteja seguro. Dessa forma, não apenas os equipamentos estão seguros, mas todas as aplicações que estão sendo executadas nesses equipamentos.

A principal ameaça que pode ter em uma rede são ataques de malwares, que estão cada vez mais presentes no ambiente corporativo. Para mitigar esse problema, a rede deve ter camadas de proteção que identifiquem essas ameaças.

O uso de ferramentas como firewall, antivírus, IPS, IDS, VPN e algumas ações como segurança de e-mail que se tornaram foco de ataques, segmentação da rede, controle de acesso, segurança de software, prevenção contra perda de dados, credenciais de login padrão e atualização de firmware.

Quando monitoramos equipamentos que estão na rede, encontramos algumas vulnerabilidades

Os switches são um dos equipamentos mais importantes na rede, pois são responsáveis pela conexão de hosts na rede e quando mal configurados podem gerar riscos para toda a infraestrutura. As vulnerabilidades encontradas em switches, muitas vezes, podem ser mitigadas através de configurações e previne contra as principais ameaças.

Depois de entender todos os riscos e utilizar da norma e dessas ferramentas listadas acima, é necessário criar uma resposta a incidentes adequada que vai diminuir os riscos que a rede está exposta e os impactos.

2. ISO/IEC 27002:2022

ISO (Organização Internacional para Padronização) e IEC (Comissão Eletrotécnica Internacional) formam o sistema especializado para padronização mundial. Organismos nacionais que são membros da ISO ou IEC participam do desenvolvimento de Normas Internacionais por meio de comitês técnicos estabelecidos pela respectiva organização para lidar com áreas específicas de atividade técnica. Os comitês técnicos ISO e IEC colaboram em áreas de interesse mútuo.

A documentação da ISO/IEC 27002:2022 foi desenvolvido para organizações de todos os tipos e tamanhos. Ele deve ser usado como uma referência para determinar e implementar controles para tratamento de riscos de segurança da informação em um sistema de gerenciamento de segurança da informação (ISMS) baseado na ISO/IEC 27001. Também pode ser usado como um documento de orientação para organizações que determinam e implementam controles de segurança da informação. Além disso, este documento destina-se ao uso no desenvolvimento de diretrizes de gerenciamento de segurança da informação específicas do setor e da organização, levando em consideração seus ambientes específicos de risco de segurança da informação.

O processo para a gestão da segurança da informação é apresentado através da ISO 27002:2022, “Código de prática para a segurança da informação” e inclui a importância de:

- Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação;
- Implementar e operar controles para gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócio da organização;
- Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (Information Security Management System - ISMS);
- Melhoria contínua baseada em medições objetivas.

Dentro da documentação da ISO 27002 existe um módulo destinado para as atividades de monitoramento. Destina-se estas atividades através de módulos como:

- Controle

Redes, sistemas e aplicativos devem ser monitorados quanto a comportamento anômalo e ações apropriadas devem ser tomadas para avaliar possíveis incidentes de segurança da informação.

- Propósito

Para detectar comportamentos anômalos e possíveis incidentes de segurança da informação.

- Orientação

O escopo e o nível de monitoramento devem ser determinados de acordo com os requisitos de negócios e segurança da informação e levando em consideração as leis e regulamentos relevantes. Os registros de monitoramento devem ser mantidos por períodos de retenção definidos

2.1. Aplicação da ISO/IEC 27002:2022

Para que um sistema de monitoramento esteja de acordo com a norma ISO 27002 deve ser considerado:

- Tráfego de rede, sistema e aplicativo de saída e entrada;
- Acesso a sistemas, servidores, equipamentos de rede, sistema de monitoramento, aplicações críticas, etc.;
- Arquivos de configuração de rede e sistema de nível crítico ou administrativo;
- Logs de ferramentas de segurança (por exemplo, antivírus, IDS, sistema de prevenção de intrusão (IPS), filtros da web, firewalls);
- Logs de eventos relacionados à atividade do sistema e da rede;
- Verificar se o código que está sendo executado está autorizado a rodar no sistema e que não foi adulterado;
- Uso dos recursos (CPU, discos rígidos, memória, largura de banda) e seu desempenho;

A organização deve estabelecer uma linha de base de comportamento normal e monitorar em relação a esta linha de base para anomalias. Ao estabelecer uma linha de base e para identificar anomalias, o seguinte deve ser considerado:

- Revisar a utilização dos sistemas em períodos normais e de pico;

- Horário habitual de acesso, local de acesso, frequência de acesso para cada usuário ou grupo de usuários;
- Encerramento não planejado de processos ou aplicativos;
- Atividade tipicamente associada a malware ou tráfego originado de endereços IP maliciosos conhecidos ou domínios de rede;
- Características de ataque conhecidas (por exemplo, negação de serviço e estouro de buffer);
- Comportamento incomum do sistema;
- Gargalos e sobrecargas (por exemplo, enfileiramento de rede, níveis de latência e jitter de rede);
- Acesso não autorizado a sistemas ou informações;
- Varredura não autorizada de aplicativos, sistemas e redes de negócios;
- Tentativas bem-sucedidas e malsucedidas de acessar recursos protegidos (por exemplo, servidores DNS, portais da web e sistemas de arquivos);
- Comportamento incomum do usuário e do sistema em relação ao comportamento esperado.

O monitoramento contínuo por meio de uma ferramenta de monitoramento deve ser usado (por exemplo, Zabbix, Cacti, Nagios). O monitoramento deve ser feito em tempo real ou em intervalos periódicos, de acordo com as necessidades e capacidades organizacionais. As ferramentas de monitoramento devem incluir a capacidade de lidar com grandes quantidades de dados, adaptar-se a um cenário de ameaças em constante mudança e permitir notificações em tempo real. As ferramentas também devem ser capazes de reconhecer assinaturas e dados específicos ou padrões de comportamento de rede ou aplicativo.

O software de monitoramento automatizado deve ser configurado para gerar alertas (por exemplo, mensagens de e-mail ou sistemas de mensagens instantâneas) com base em limites predefinidos. O sistema de alerta deve ser ajustado e treinado na linha de base da organização para minimizar falsos positivos. O pessoal deve ser dedicado a responder aos alertas e deve ser devidamente treinado para interpretar com precisão os potenciais incidentes. Deve haver sistemas e processos redundantes para receber e responder a notificações de alerta.

Além disso a norma ISO recomenda possíveis aprimoramentos ao monitoramento no intuito de aplicar ainda mais segurança aos processos, alguns aprimoramentos recomendados são:

- Alavancar sistemas de inteligência de ameaças;
- Alavancar os recursos de aprendizado de máquina e inteligência artificial;
- Realizar uma série de avaliações técnicas de segurança (por exemplo, avaliações de vulnerabilidade, testes de intrusão, simulações de ataques cibernéticos e exercícios de resposta a incidentes) e usando os resultados dessas avaliações para ajudar a determinar linhas de base ou comportamento aceitável;
- Usar sistemas de monitoramento de desempenho para ajudar a estabelecer e detectar anomalias;
- Aproveitamento de logs em combinação com sistemas de monitoramento.

3. ZABBIX

Como mencionado no capítulo onde é tratado a Norma ISO 27002 voltado ao capitulo de monitoramento, existem informações pertinentes a serem monitoradas, afim de direcionar o sistema de monitoramento a captação das informações mais relevantes.

A ferramenta Zabbix é capaz de coletar diversas informações disponibilizadas pelo host, e essa coleta pode ocorrer de várias formas, como com uso de um Agente Zabbix no host ou com uso do protocolo SNMP, sendo esses os métodos mais comuns para realizar essa coleta de dados.

Em casos com redes mais complexas ou populosas o Zabbix também é capaz de trabalhar com serviço de Proxy para realizar a comunicação com os hosts.

De maneira geral o Zabbix opera com um “Zabbix Server”, o qual fica responsável por requisitar todas as informações dos hosts com ou sem agente, sendo assim o encarregado de enviar as requisições de dados.

Uma vez que os dados dos hosts chegam ao *Server,* essas informações são armazenadas em um banco de dados (MySQL, Oracle ou PostgreSQL) e então processadas a partir de triggers criados pelo administrador.

A seleção de dados que são coletados pelo servidor se dá pelo template, onde é possível configurar o modo como essa requisição será feita (protocolo SNMP, Agente nativo, etc.) e junto ao template são criados os triggers mencionados anteriormente, os quais podem gerar ações como envio de e-mails, notificações e até envio de comando aos hosts quando possível.

O “Zabbix Server” pode trabalhar em conjunto com “Zabbix Proxy”, esse recurso permite o monitoramento de redes distintas ao mesmo tempo que reduz a carga de processamento do próprio server.

Além do “Zabbix Server”, o sistema trabalha com os “Zabbix Agents”, que se trata de uma ferramenta instalada no host, a qual coleta os dados dele e envia ao server configurado.

Há casos em que não é possível a instalação de um agente, como o caso de switchs, impressoras, etc., portanto nesse tipo de situação os hosts são do tipo “*agentless*” e tais hosts são monitorados normalmente por outros meios, como por exemplo, através do protocolo SNMP.

O “Protocolo Simples de Gerência de Rede” (SNMP) foi desenvolvido com foco em realizar o monitoramento de equipamentos conectados a uma rede IP. Para

uso junto ao Zabbix há duas partes de interesse no protocolo, os comandos padrões, que retornam algumas informações básicas como latência, perda de pacote e disponibilidade.

A segunda parte que consiste nos comandos gerados pelo fabricante, denominados como *enterprises,* fornecem outras informações sobre o dispositivo, como uso de CPU, IP atual, MAC Address, uso da memória, etc.

Uma vez que os templates e triggers são criados e atribuídos aos dispositivos a serem monitorados, as informações de ocorrências começam a aparecer no dashboard básico do próprio Zabbix. Pelo fato de o Zabbix ser um software open source, existem ferramentas extras que interagem com ele, como o caso do Grafana uma ferramenta que foi utilizada no projeto para melhorar a experiência do usuário e que será melhor descrita no próximo capítulo.

3.1. Implementações no Zabbix

Conhecendo melhor a ferramenta é possível abordar os itens trabalhados no Zabbix pela equipe de segurança afim de incrementar o monitoramento da rede do Campus da FACENS.

A princípio foi entregue um servidor Zabbix de testes com diversos hosts cadastrados pela equipe de T.I., sendo em sua maioria, *Access Point's* (AP's), isto é, antenas WiFi, e que já possuíam um template com triggers e outros Hosts como switch's e impressoras sem um template para coleta de dados.

Com base na ISO 27002 e nas especificações feitas pela equipe de T.I. da FACENS, foram determinadas as principais informações a serem coletadas:

- Uso da CPU;
- Disponibilidade;
- Latência;
- Perda de pacote.

E para tais informações gerar triggers de modo a alertar anomalias. Além dessas, outras informações foram inclusas em cada template, informações como Versão de Firmware, MAC Address, Uptime e etc.

Nome	Triggers	Chave ▲	Intervalo	Histórico	Estatísticas	Tipo
Gateway		enterprises.2011	1m	90d		SNMP agent
Versão Firmware		Firmware	1m	90d		SNMP agent
Memória Total		h3cEntityExtMemSize	1m	90d	365d	SNMP agent
Utilização de CPU	Triggers 1	hwLswSysCpuRatio	1m	90d	365d	SNMP agent
FACENS - ICMP: Disponibilidade ICMP	Triggers 2	icmpping	1m	7d	90d	Monitoração simples
FACENS - ICMP: Perda de pacote	Triggers 1	icmppingloss	1m	7d	90d	Monitoração simples
FACENS - ICMP: Latência	Triggers 1	icmppingsec	1m	1w	365d	Monitoração simples
Mac Address		ifPhysAddress	1m	90d		SNMP agent
IP		ipAdEntAddr	1m	90d		SNMP agent
Time to Live		ipDefaultTTL	1m	90d	365d	SNMP agent
Descrição		sysDescr	1m	2w		SNMP agent
Localização		sysLocation	1m	90d		SNMP agent
Hostname		sysName	1m	2w		SNMP agent
Uptime		sysUpTimeInstance	1m	90d	365d	SNMP agent

Figura 1 – Exemplo de template.

Assim, tendo em vista tais definições e o escopo do projeto, descrito no Termo de Abertura de Projeto (TAP), foram criados templates para coletar informações de modelo de Switch presente no laboratório de Informática de modo que foi necessário realizar a busca dos Identificadores de Objetos (OID's) de cada modelo de equipamento afim de coletar as informações corretas.

Foram levantados 5 modelos distintos e Switchs e mais um modelo de impressora no laboratório de informática, tais equipamentos foram listados para facilitar a busca pelas suas OID's.

Fabricante	Modelo	Tipo
DELL	X1052	Switch
HP	V1905-48	Switch
3COM	2250/SFP	Switch
UNIFI	US-48-750W	Switch
DELL	N1524P	Switch
VERSALINK	C7020	Impressora

Tabela 1 – Modelos de equipamentos

Ao todo foram criados 7 templates para os diversos modelos de Switch's presentes no campus, onde eles foram testados em seus respectivos hosts para validar se os OID's utilizados estavam corretos.

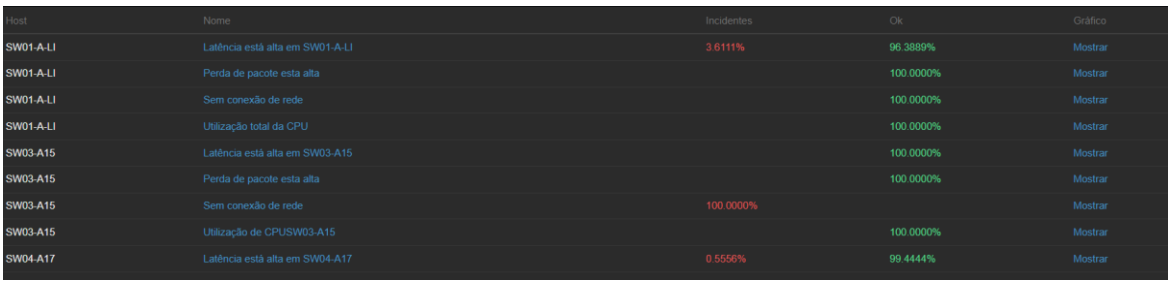
Nome ▲	Hosts	Itens	Triggers	Gráficos	Dashboards	Descoberta	Web
LENOVO - SNMP - IMPRESSORAS - VERSALINK - C7020	Hosts 1	Itens 19	Triggers	Gráficos	Dashboards	Descoberta	Web
LENOVO - SNMP - SWITCHES - DELL - SERIE - N15	Hosts 6	Itens 17	Triggers 5	Gráficos 1	Dashboards	Descoberta	Web
LENOVO - SNMP - SWITCHS - DELL - SERIE - X10	Hosts 19	Itens 30	Triggers 6	Gráficos 1	Dashboards	Descoberta	Web
LENOVO - SNMP - SWITCHS - DELL - SERIE - X10 - VER WIFI	Hosts 2	Itens 32	Triggers 6	Gráficos 1	Dashboards	Descoberta	Web
LENOVO - SNMP - SWITCHS - HP - SERIE - V1905	Hosts 11	Itens 14	Triggers 5	Gráficos 1	Dashboards	Descoberta	Web
LENOVO - SNMP - SWITCHS - HP3COM - SERIE - 2250	Hosts 4	Itens 18	Triggers 6	Gráficos 1	Dashboards	Descoberta	Web
LENOVO - SNMP - SWITCHS - UNIFI - SERIE - US48	Hosts 8	Itens 26	Triggers 6	Gráficos 1	Dashboards	Descoberta	Web

Figura 2 – Lista de templates criados.

Uma vez que todos os templates foram criados e associados a seus devidos hosts todas as ocorrências relacionadas a eles começaram a aparecer no dashboard básico do Zabbix, assim como já mencionado anteriormente.

Todavia, além das notificações relacionadas aos equipamentos dos templates criados haviam as demais notificações, sobre status de AP's, servidores, etc. Afim de selecionar melhor a exibição foi proposta a elaboração de um dashboard com Grafana.

Além do dashboard global, o Zabbix possui outras funções interessantes que podem ser exploradas, como o gerador de relatório, o qual exibe uma taxa de incidentes em relação a cada trigger e para cada equipamento.



Host	Nome	Incidentes	Ok	Gráfico
SW01-A-LI	Latência está alta em SW01-A-LI	3.6111%	96.3889%	Mostrar
SW01-A-LI	Perda de pacote esta alta		100.0000%	Mostrar
SW01-A-LI	Sem conexão de rede		100.0000%	Mostrar
SW01-A-LI	Utilização total da CPU		100.0000%	Mostrar
SW03-A15	Latência está alta em SW03-A15		100.0000%	Mostrar
SW03-A15	Perda de pacote esta alta		100.0000%	Mostrar
SW03-A15	Sem conexão de rede	100.0000%		Mostrar
SW03-A15	Utilização de CPUSW03-A15		100.0000%	Mostrar
SW04-A17	Latência está alta em SW04-A17	0.5556%	99.4444%	Mostrar

Figura 3 – Relatório do Zabbix.

Sendo possível planejar possíveis manutenções com base nos incidentes que ocorreram em maior proporção.

3.2. Monitoramento de ataques através do zabbix

Através do zabbix, é possível fazer o monitoramento de diversos ataques contra os dispositivos cadastrados em monitoramento, o que é de extrema importância

para a confidencialidade, integridade e disponibilidade das informações e serviços que estão em funcionamento através dos equipamentos de rede.

Para fazer o monitoramento dos ataques primeiramente é necessária a criação de templates que possuam os itens que são afetados por cada ataque em específico que se deseja monitorar. Por exemplo, para ataques de DOS e DDOS, que são extremamente comuns, é necessário o uso de templates que tenham como itens a quantidade de bytes que estão sendo trafegados na rede por segundo e também a quantidade de requisições e acessos a um determinado equipamento e servidor por segundo.

Com os templates configurados corretamente e com os itens certos para a detecção dos ataques que se deseja monitorar, o próximo passo é a criação de triggers, principalmente para os itens mais importantes, com o intuito de que o zabbix faça alguma ação para alertar o administrador da rede sobre o possível ataque. Um ponto muito importante é quando um trigger for acionado, antes é preciso configurar o zabbix para que envie um alerta por e-mail como exemplo, informando o responsável sobre o possível ataque que está sendo feito no equipamento específico da rede. Neste e-mail é interessante relatar sobre qual é o possível ataque que está sendo realizado assim como indicar a classificação da severidade, qual o atacante e também possíveis correções e métodos a serem executados para tentar eliminar o ataque.

4. GRAFANA

O monitoramento da rede facilita correções, mas é necessário que as informações estejam exibidas de forma clara. Para isso, o uso de ferramentas que deixam os dados coletados em forma gráfica, facilita a visualização e compreensão de possíveis falhas nos sistemas.

O Grafana é um software gratuito e de código aberto, de fácil integração com diversas ferramentas, como Zabbix e MySQL, que possibilita a visualização de dados através de gráficos e dashboards dinâmicos.

O uso do Grafana é importante para gestão de indicadores e métricas, além de trazer praticidade e agilidade, ajudando na tomada de decisões. Quando utilizado com uma ferramenta de monitoramento, como Zabbix, é possível utilizar os dados do Zabbix, como grupo de equipamentos, hosts e os itens que estão sendo

monitorados para gerar painéis dinâmicos e saber se algum equipamento está com problemas ou apresentando um comportamento diferente.

Entre os equipamentos que é possível visualizar no Grafana estão servidores, switches, firewall e qualquer outro equipamento que possa ser monitorado pelo Zabbix. Além disso é possível visualizar informações de outros softwares e de bancos de dados.

Como vantagem da utilização dessa ferramenta, além de gerar indicadores, o recurso é em tempo real, permitindo que as informações sejam vistas no momento exato, ajudando esse acompanhamento do setor de TI.

4.1. Implementações no Grafana

Foi entregue para a equipe o acesso ao Grafana, já utilizado pela Facens, para entendimento de como os equipamentos são visualizados pelo Grafana e quais os principais itens monitorados que são importantes de serem exibidos.

No Grafana, a equipe inseriu mais um dashboard, contendo todos os grupos de hosts do Zabbix e todos os hosts. No dashboard há um painel com todos os problemas que estão acontecendo no campus em tempo real. Abaixo desse painel, há outras informações importantes sobre os equipamentos, como latência, uso de CPU, disponibilidade ICMP e uptime.

A visualização dos equipamentos é separada por grupos de hosts. Os itens que seriam monitorados foram escolhidos pela relevância das informações.

A latência e a disponibilidade ICMP são importantes para saber a qualidade de transmissão da rede e se há disponibilidade do equipamento no momento. O uso de CPU indica se o equipamento está nos níveis adequados de consumo ou se há algum aumento podendo indicar um problema, como mal funcionamento ou ataque. O uptime indica o tempo de funcionamento do equipamento ligado.

5. SEGURANÇA DE REDES E APLICAÇÕES WEB

Para realizar a proteção de sistemas web é de extrema importância o conhecimento das vulnerabilidades mais recorrentes para o tipo de aplicação que está sendo desenvolvida e também as ações necessárias para a correção de possíveis brechas de segurança. Diante dessas informações, uma organização muito conhecida e responsável por desenvolver projetos de segurança para aplicações web é a OWASP (Open Web Application Security Project), uma

fundação sem fins lucrativos cujo objetivo é melhorar a segurança de softwares, sendo a maior organização sem fins lucrativos do mundo a atuar nesta área.

A OWASP conduz diversos projetos ao redor do tema segurança de software, como o Zed Attack Proxy, Security Knowledge Framework, Juice Shop, WebGoat, OWASP Top Ten, entre outros.

5.1. O projeto OWASP Top Ten

O projeto OWASP Top Ten é um relatório desenvolvido por especialistas em segurança da informação do mundo todo. Tem como objetivo, listar as 10 vulnerabilidades mais críticas de segurança em aplicações web. Essas vulnerabilidades são definidas por ordem de importância e revisadas em média a cada três anos.

É importante sempre verificar o projeto OWASP Top Ten para tomar conhecimento de quais as vulnerabilidades que estão ocorrendo de forma mais frequente nas aplicações web, assim como ter o conhecimento de como os cibercriminosos utilizam essas brechas de segurança para explorarem diversos sistemas e como corrigi-las.

5.2. Ferramentas de Segurança

No desenvolvimento de software é comum que o desenvolvedor não esteja ciente da importância do ciclo de desenvolvimento seguro de um sistema. Para auxiliar nas criações de aplicações mais seguras, é importante a utilização de ferramentas de SAST, DAST e IAST, responsáveis por contribuir de forma bastante efetiva para um software mais seguro, com menos brechas de segurança que os cibercriminosos consigam utilizar para realizarem ataques na aplicação.

5.3. Ataques de Malwares

Com o advento do trabalho remoto, causado pela pandemia do COVID-19, foi observado um grande aumento de crimes cibernéticos e ataques de malware. O impacto gerado por estes ataques é devastador em termos financeiros e para a imagem das empresas.

Ataques de ransomware estão relacionados a vazamento de dados, perca de acesso a arquivos e informações relevantes. Segundo a IBM Security, em 2021,

os ataques de ransomware geraram, globalmente, em média, um prejuízo de 4,62 milhões de dólares por ataque.

Os custos de um ataque envolvem o tempo que se leva para detectar o ataque, as ações necessárias para conter os danos, os negócios perdidos, o dano à reputação, o tempo que a empresa fica impossibilitada de continuar suas operações, além da perda financeira. Em 2021, demorou-se em média 287 dias para detectar e conter um vazamento de dados (IBM SECURITY, 2021).

No Brasil foram registrados diversos ataques cibernéticos a empresas. Um caso famoso foi o da empresa do setor alimentício JBS S.A., que foi atacada pelo ransonware REvil e pagou o resgate solicitado no valor de 11 milhões de dólares (EXAME, 2021). O custo médio de vazamento de dados no Brasil, em 2021, foi de 1,08 milhões de dólares por ataque (IBM SECURITY, 2021).

Desta forma fica evidente o aumento dos riscos de estar exposto a internet e a correlação do aumento de ataques com a pandemia e o trabalho remoto. Com isto, é necessário que as empresas busquem aumentar a sua segurança e que os desenvolvedores de software adotem práticas de codificação mais seguras.

Modelos de trabalho, pesquisas, relatórios e informações relacionadas à segurança da informação podem ser consultadas na instituição Open Web Application Security Project.

5.4. Segurança de Rede

Sem dúvidas a segurança das redes de uma empresa é fundamental e precisa ser priorizada, pois através de uma rede mal configurada, sem as devidas proteções necessárias, muitos ataques serão bem sucedidos podendo desta forma comprometer a empresa como um todo devido a infecção por malwares do tipo ransomwares e worms, os quais podem se espalhar através de um computador infectado para a rede inteira, podendo ser devastador para os negócios, deixando operações inoperantes, levando a prejuízos financeiros, vazamento e perdas de dados e manchando o nome da empresa.

Para que os problemas listados sejam em grande parte evitados é importante a utilização de firewalls, segurança de e-mails, antivírus e antimalware, segmentação da rede, controle de acesso, segurança do software, prevenção contra perda de dados, sistemas de prevenção contra invasão, vpn, trocar as

credenciais de login padrão dos equipamentos de rede, atualização do firmware, entre outros.

5.4.1. Firewall

São equipamentos de segurança que podem ser físicos ou no formato de softwares, responsáveis por filtrar e barrar tráfegos de rede definidos através de regras, deixando que somente sejam enviadas e recebidas conexões que estejam permitidas nas regras configuradas do firewall.

Existem diversos tipos de firewall, são eles: packet-filtering firewalls, next-generation firewalls (NGFW), Proxy firewalls, Network Address Translation Firewalls e Stateful multilayer inspection firewalls.

Os firewalls são de extrema importância para a segurança da rede já que quando bem configurados, fazem o filtro e bloqueiam tráfegos de rede suspeitos, eliminando desta forma diversos ataques que passariam despercebidos pela rede.

5.4.2. Segurança de e-mails

E-mails se tornaram uma ferramenta de ataque extremamente funcional por parte dos cibercriminosos, devido aos usuários muitas das vezes não possuírem o conhecimento necessário sobre e-mails falsos e malwares. Diante desse conhecimento os hackers criminosos se passam por empresas confiáveis e utilizam de diversas técnicas de phishing e envio de anexos contaminados para suas vítimas, que muitas das vezes abrem o e-mail e realizam a ação que os atacantes descrevem.

5.4.3. Antivírus

Antivírus são softwares de extrema importância nos computadores, sendo capazes de proteger, detectar e remover as ameaças encontradas. Somente com a utilização de um bom antivírus, diversas infecções são detectadas e bloqueadas, desta forma são considerados indispensáveis no monitoramento de computadores de uma empresa, que a todo tempo são alvos de diversos malwares, devido aos usuários baixarem arquivos de fontes desconhecidas, correndo o risco de por exemplo, espalhar um malware do tipo worm na rede inteira da empresa.

5.4.4. Segmentação da rede

Faz a divisão da rede em sub-redes com o intuito de promover uma maior segurança para cada uma delas, oferecendo um maior controle sobre o tráfego da rede, reduzindo a superfície de ataque e impedindo movimentos laterais, que são amplamente utilizados por malwares do tipo worm, por exemplo. Fazendo com que por meio de um determinado computador infectado, o malware consiga acesso a rede ou então explore determinada vulnerabilidade presente naquele host e se espalhe para outros computadores.

5.4.5. Controle de acesso

São controles de segurança que envolvem permissões para acessar determinados lugares ou equipamentos. Desempenham um papel fundamental para impedir que uma pessoa que não possua a permissão necessária acesse determinado local.

Empresas que não possuem controle de acesso, estão expostas a roubos e infiltrações por parte de hackers criminosos, pois desta forma conseguem por exemplo acessar determinados ambientes com informações sigilosas que deveriam ser controlados e protegidos contra pessoas não autorizadas.

5.4.6. Segurança do Software

A segurança no desenvolvimento de softwares evita diversos problemas de performance, custos, além de evitar brechas que cibercriminosos podem vir a explorar.

No desenvolvimento de software, boas práticas de código e a realização de testes de segurança devem ser seguidos desde o início, pois quanto mais cedo se detecta uma vulnerabilidade, menor é o gasto para corrigi-la, além de não deixar a aplicação ir para produção com brechas de segurança que poderiam ser facilmente resolvidas se fossem feitos testes de análise de código logo no início do desenvolvimento.

Por mais que não tenham sido feitos testes de segurança na aplicação no período de desenvolvimento, é possível ainda fazer testes de segurança dinâmicos com a aplicação em execução. O problema é que normalmente neste estágio, as vulnerabilidades encontradas podem acabar custando mais caro para serem corrigidas, porém é preferível a realização desses testes do que deixar a aplicação exposta à internet contendo vulnerabilidades que são facilmente exploradas por

atacantes, levando a diversos prejuízos relacionados a serviços que precisem ou fiquem offline devido aos ataques, financeiro e de reputação da empresa, como por exemplo, os dados de seus clientes vazados.

5.4.7. Prevenção contra perda de dados

De extrema importância para a proteção dos dados da empresa e dos seus clientes que com ataques de hackers criminosos ou até mesmo dos próprios funcionários da organização, tendem a obter acesso a informações confidenciais e divulgá-las expondo a empresa e os usuários. Esse tipo de situação pode causar prejuízos gravíssimos para a empresa que é a responsável pelos dados de seus clientes, infligindo diretamente na LGPD e causando uma grande perda financeira e de imagem.

Para evitar tais perdas é importante a utilização de um software de prevenção contra perda de dados, que funciona de forma que o usuário consiga escolher quais os arquivos ele deseja fazer a proteção por meio de regras, indicando informações que são confidenciais por exemplo, para que não possam ser compartilhadas, impedindo que informações internas da empresa sejam expostas.

5.4.8. Sistemas de prevenção contra intrusão (IPS) e detecção de intrusão (IDS)

Ambos os sistemas são complementares, enquanto que o IDS faz a detecção de uma tentativa de intrusão, o IPS protege de fato aquele sistema contra a invasão. Utilizam diversas métricas para fazer a proteção do sistema, normalmente definidas pelo administrador da rede.

Esses sistemas de proteção são muito importantes e eficientes fazendo com que ataques sejam barrados logo no início ao tentar entrar na rede, alertando e fazendo a prevenção contra os ataques além de proporcionar que a rede não sofra atrasos na comunicação durante a atuação desses sistemas.

5.4.9. VPN

Se tratando de segurança na comunicação de um host a um servidor, pode-se fazer uso de VPNs as quais são responsáveis pela proteção das trocas de informações entre as partes conectadas, evitando que ocorram interceptações no

tráfego de rede e que o provedor ISP não consiga rastrear e ter o conhecimento das informações trafegadas no endereço IP de um host em específico.

VPNs são de extrema importância em redes públicas, pois nesses casos não há como saber se existe algum tipo de monitoramento do tráfego gerado, evitando que as informações trafegadas sejam vistas por usuários conectados na mesma rede Wi-Fi.

5.4.10. Credenciais de login padrão nos equipamentos de rede

Uma falha muito comum em diversas empresas é a utilização de credenciais de login padrão nos equipamentos da rede, fazendo com que criminosos cibernéticos ou até mesmo funcionários da própria empresa possam ter acesso a dispositivos sem a menor dificuldade, visto que credenciais padrão dos equipamentos são facilmente encontradas, ocasionando em brechas críticas de segurança que podem comprometer toda a rede da empresa se ocorrerem acessos indevidos sem a permissão necessária.

Todos equipamentos de rede precisam de credenciais de login novas contendo um grande número de caracteres assim como caracteres especiais para reforçar a segurança de acesso e dificultar ataques de força bruta, que fazem a utilização de listas contendo diversas senhas padrão.

5.4.11. Atualização do firmware de equipamentos de rede

Muitas das vezes equipamentos de rede possuem firmware com versões desatualizadas e vulneráveis, levando a um possível invasor conseguir injetar ou esconder um malware no equipamento com firmware desatualizado.

As atualizações de firmwares são de extrema importância, portanto assim que o fabricante disponibiliza uma nova versão, os usuários precisam fazer o download e instalar cuidadosamente, pois uma mudança que ocorra no código do firmware é capaz de deixar o host inoperante.

6. VULNERABILIDADES NOS SWITCHS

O switch é um equipamento que conecta os equipamentos da rede para que possam trocar dados entre si. O switch recebe os dados do computador de origem e redireciona para o computador de destino.

Os switches podem apresentar vulnerabilidades, quando fazem o uso de senha padrão, permitem escrita, estão configurados de forma padrão ou mal configurados. O uso de senhas padrão permite o acesso de outras pessoas não autorizadas, por se tratar de uma senha fácil, e esse acesso pode levar a informações do switch.

Alguns switches podem estar configurados para escrita e podem ser enviados scripts, até pelo Zabbix, alterando as configurações.

A configuração padrão do switch também se torna um risco, pois é necessário adequar o switch a rede.

A configuração incorreta se torna um risco, pois alguma configuração importante pode ser deixada de lado e pode ser necessária para a segurança da rede. Um dos exemplos de configuração incorreta é a lista de acesso permitida para o switch, os protocolos e a comunidade SNMP.

Abaixo estão listados alguns ataques em switches:

- TLStorm: conjunto de cinco vulnerabilidades que permitem execução remota de código (RCE) exploráveis pela rede, permitindo movimento lateral para dispositivos alterando o comportamento do switch, exfiltração de dados do tráfego de rede ou informações confidenciais da rede interna para a Internet e bypass dos protocolos de login.
- MAC Spoofing (falsificação de endereço MAC): troca da tabela CAM que tem os endereços MAC, por uma que aponta para o MAC do atacante.
- CAM Overflow (estouro da memória CAM): memória CAM possui tamanho limitado, enche a memória e o switch se comunica com todas as portas, se comporta como hub.
- DHCP Starvation (ataques serviço DHCP): envia diversas requisições DHCP e esgota os IPs.
- Rogue DHCP Server (DHCP falsos): envia DHCP falsos possibilitando um Man in the middle.
- ARP Spoofing (falsificação de endereço MAC): falsifica o endereço MAC e IP, gerando negação de serviço e Man in the middle.
- Ataques a VLAN e STP: utiliza pacotes multicast e broadcast, com acesso a informações (sniffing ou espionagem) e cpu em 100% comprometendo o funcionamento.

Existem algumas formas de evitar essas vulnerabilidades:

- Port security: limita número de endereços MAC aprendidos pela porta do switch ou fixar o MAC;
- BPDU guard: protege as portas do switch detectando BPDUs recebidos em locais não permitidos bloqueando a porta;
- Root guard: controle de porta protegendo a topologia do STP;
- Dynamic ARP inspection: previne o spoofing analisando as características dos hosts conectados às portas dos switches;
- IP source guard: protege a rede contra a falsificação;
- 802.1x: autentica usuários e permite que somente quadros devidamente autenticados sejam enviados na rede;
- DHCP snooping: previne que servidores DHCP piratas injetem informações falsas em clientes de rede;
- Storm control: limita a quantidade de tráfego broadcast ou multicast enviados pelos switches na rede;
- Access control lists: controle de acesso.

Alguns fabricantes como HP, 3COM e DELL possuem em seus manuais de referência informações sobre como fazer essas configurações de segurança.

7. RESPOSTA A INCIDENTES

A resposta a incidentes pode ser compreendida como o processo de uma determinada empresa ou organização de reagir a ameaças que surgem nos dias atuais, devido à alta crescente da utilização de recursos tecnológicos, como ataques cibernéticos, vazamentos de dados, vulnerabilidades de softwares e violações de acessos, e tem por objetivo identificar tais ameaças, garantir o registro das atividades relacionadas ao incidente, avaliar os impactos proporcionados por tais incidentes, realizar a comunicação do incidente a quem é de interesse, escalonar o incidente para as pessoas capacitadas a tratarem o problema, e solucionar o incidente, mantendo todas as ocorrências devidamente registradas e catalogadas.

De acordo com o capítulo 5.24 da norma ISO/IEC 27002:2022, as organizações devem realizar um planejamento e preparação para lidar com incidentes relacionados à segurança da informação, definindo funções e responsabilidades que cada membro deve exercer durante o gerenciamento de um incidente, a fim de que se garanta uma rápida e eficaz resposta a tais incidentes.

Ainda de acordo com o capítulo 5.24:

- Deve-se elaborar um método comum para relato de eventos que possam comprometer a segurança da informação;
- Estabelecer processos de gerenciamento de tais eventos, de modo que os registros corroborem para análises e casos futuros, servindo também de aprendizado para a equipe de resposta a incidentes;
- Permitir que pessoas competentes lidem com os eventos, garantindo a estes também documentação necessária e treinamentos periódicos sobre a área.

Tendo um efetivo sistema de registro de eventos de segurança de informação, através do monitoramento, de logs, ou de relatos dos usuários, deve-se avaliar cada um desses eventos a fim de categorizá-los ou não como incidentes de segurança da informação, permitindo que determinados incidentes sejam priorizados, de acordo com a categorização realizada.

Com os eventos devidamente registrados e categorizados, deve-se realizar a resposta a incidentes, que atua de forma corretiva, e que está relacionado às propriedades de confidencialidade, integridade e disponibilidade, buscando

responder de forma rápida e eficaz aos incidentes ocorridos, e se possível, recuperar dados que possam ter sido comprometidos.

Os incidentes devem ser respondidos por uma equipe com as competências necessárias para tratá-los, e tal resposta deve incluir:

- Os sistemas afetados por esse incidente, caso as consequências possam se espalhar;
- Coleta de evidências;
- Escalonamento das ações a serem tomadas, com base nas atividades de gerenciamento de incidentes; garantir que haja um registro de todas as atividades relacionadas à resposta, de modo que estes registros possam ser analisados posteriormente;
- Comunicação a todas as partes a quem é de interesse sobre o incidente ocorrido, bem como qualquer detalhe relevante, seguindo a técnica de controle need-to-know, garantindo a disponibilidade de uma informação que é necessária para as funções destes que foram comunicados;
- Cooperar com diversas entidades, internas ou externas, como autoridades, grupos de interesses, fóruns, fornecedores e clientes, a fim de garantir uma resposta efetiva e ajudar a mitigar as consequências causadas a outras organizações;
- Encerramento e registro formal do incidente, quando o mesmo for resolvido;
- Realização de análise forense de segurança da informação, caso necessário;
- Realização de análise pós-incidente, para identificação da causa raiz;
- Identificação e gerenciamento de vulnerabilidades que possam ter causado, ou contribuído para o incidente sárias para tratá-los, e tal resposta deve incluir:

Com a resposta efetuada, deve-se utilizar o incidente como fonte de aprendizado e de melhorias na segurança da informação, pois através deste evento tratado, pode-se compreender melhor os pontos fracos e assim obter um melhor controle no gerenciamento destes incidentes.

8. CONCLUSÃO

O uso de sistemas da informação, softwares e hardwares nas empresas se faz cada vez mais utilizável. Com o aumento das redes em uma empresa, aquisição de equipamentos e o aumento no número de funcionários o uso de novas tecnologias, metodologias e normas se faz necessário.

Com base na norma ISO/IEC 27002:2022 vemos métricas e parâmetros recomendados para a devida aplicação de segurança da informação na empresa. O uso de ferramentas como o Zabbix e o Grafana para o setor de monitoramento de redes também se faz necessário para garantir que a disponibilidade dos equipamentos, administração e o controle dos equipamentos instalados seja efetiva.

Com o intuito de aplicar segurança da informação na empresa, além de seguir a norma 27002 dentre outras normas voltadas para a área, também é necessário entender o funcionamento dos equipamentos utilizados na empresa, como switchs, servidores, etc. para que os administradores da rede possam pesquisar e entender as possíveis vulnerabilidades dos equipamentos e da conexão de rede da empresa, é preciso ter conhecimento técnico deles só assim é possível traçar uma linha de base para começar a se adequar as normas de segurança da informação e garantir que a confidencialidade, integridade e disponibilidade dos equipamentos e das informações da empresa estejam devidamente ativas e seguras de ataques maliciosos.

Tendo conhecimentos de seus equipamentos e as vulnerabilidades da empresa, se inicia o processo de implementar metodologias de gerenciamento e controle, sempre com o intuito de garantir um funcionamento eficaz dos serviços aplicando conceitos e práticas da segurança da informação.

Continuando o processo de adequar a empresa e/ou o setor organizacional, tendo em vista que já foi aplicado as metodologias e ferramentas utilizadas para garantir a segurança das informações, é necessário criar respostas aos incidentes antes, durante e depois de ocorrerem, para garantir de forma preditiva, preventiva e corretiva que o incidente, ataque malicioso, ou imperícia de algum funcionário cause algum dano ou interrompa um processo.

Concluindo, para implementar corretamente segurança da informação nas empresas é necessário estudo, organização e treinamento, só assim a empresa, principalmente o setor de T.I., conseguem garantir que os três pilares da

segurança da informação, confidencialidade, integridade e disponibilidade assim como a LGPD (Lei Geral da Proteção de Dados) seja devidamente implementada garantindo maior eficiência, gestão e controle do uso de dados, equipamentos e informações.

9. REFERÊNCIAS BIBLIOGRAFICAS

Cisco. O que é segurança de rede? Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html. Acesso em 26 jul. 2022

CrowdStrike. 2022 Global Threat Report. CrowdStrike, 2022. Acesso em 26 jul. 2022.

Deep Instinct. Cyber Threat Landscape Report 2022. Deep Instinct, 2022. Acesso 26 jul. 2022.

Exame. JBS pagou US$ 11 milhões em resgate a autores de ataque ransomware. Disponível em: https://exame.com/tecnologia/jbs-pagou-us-11-milhoes-a-autores-de-ataque-de-ransomware/. Acesso em 26 jul. 2022.

Forcepoint. What is a Firewall? Disponível em: https://www.forcepoint.com/pt-br/cyber-edu/firewall. Acesso em 26 jul. 2022.

FOUNDATION, OWASP, 2021. OWASP Top Ten. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em 26 jul. 2022

HINTZBERGEN, Jule et al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Brasport, 2018. Acesso em 26 jul. 2022.

Kaspersky. O que é uma VPN e como funciona? Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn. Acesso em 28 jul. 2022.

Malwarebytes. Antivírus. Disponível em: https://br.malwarebytes.com/antivirus/ Acesso em 27 jul 2022.

Objective. Como garantir a segurança no desenvolvimento de software? Disponível em: https://www.objective.com.br/insights/seguranca-no-desenvolvimento-de-software/ Acesso em 27 jul. 2022.

Ogasec. O que é um Sistema de Prevenção de Intrusão (IPS)? Disponível em: https://ogasec.com/blog-ogasec/2018/6/5/o-que-um-sistema-de-preveno-de-intruso-ips. Acesso em 28 de jul. 2022.

OWASP. Source Code Analysis Tools. Disponível em: https://owasp.org/www-community/Source_Code_Analysis_Tools. Acesso em: 26 jul. 2022.

OWASP. Vulnerability Scanning Tools. Disponível em: https://owasp.org/www-community/Vulnerability_Scanning_Tools. Acesso em: 26 jul. 2022.

OWASP. OWASP DevSecOps Guideline - v-0.2. Disponível em: https://owasp.org/www-project-devsecops-guideline/latest/02c-Interactive-Application-Security-Testing. Acesso em: 26 jul. 2022.

Proofpoint. What is Email Security? Disponível em: https://www.proofpoint.com/us/threat-reference/email-security. Acesso em 26 de jul. 2022.

Vantix. 10 razões pelas quais sua empresa precisa de DLP – Data Loss Prevention. Disponível em:https://www.vantix.com.br/blog/ciberseguranca/empresa-precisa-dlp/. Acesso em 28 jul de 2022.

VMware. Segmentação de rede. Disponível em: https://www.vmware.com/br/topics/glossary/content/network-segmentation.html Acesso em 27 jul. 2022.

Atlassian. The 7 stages of effective incident response. Disponível em: https://www.atlassian.com/br/incident-management/incident-response

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005. Acesso em 26 jul. 2022.