Assignment 3

Plano de Segurança

Marco Querido - 1220268

Pedro Oliveira - 1220495

Mestrado em Engenharia Informática

Docentes

Nuno Pereira, Pedro Rodrigues, Jorge Pinto Leite, António Costa ([nap | dcr | jpl | acc] @isep.ipp.pt)

Índice

Abstract

O mundo está em constante evolução tecnológica. Todos os anos são lançados novos modelos de smartphones, computadores pessoais, smartwatches ou até televisões, e o consumo destes produtos é enorme.
Depois do impacto do Covid-19 no mundo, e do número de ataques informáticos a empresas e singulares divulgados através dos media, a segurança informática teve uma maior importância na conceção e desenvolvimento de novas tecnologias, e cada vez mais é uma preocupação atualmente.
Este documento tem como propósito descrever um plano de segurança para uma instituição de saúde portuguesa que armazena toda a informação relacionada com o Covid-19, incluindo as notícias sobre a doença, e o plano de vacinação de cada cidadão. A informação deve ser classificada e acessível via página web. A infraestrutura do sistema já está implementada e consiste num servidor de autenticação, um servidor web e um servidor de ficheiros. Os canais de comunicação são públicos, e não está planeada a criação de canais privados.
No documento serão evidenciadas políticas, standards, guidelines e procedimentos para desenvolver um plano de segurança.

Keywords: dados, encriptação, acessos, permissões, token, VPN.

Políticas

Definição: Afirmação generalista sobre uma organização e os seus objetivos, âmbito e crenças. Devem ser obrigatoriamente seguidas e cumpridas, caso contrário são emitidas ações disciplinares. As seguintes políticas visam auxiliar na gestão da segurança da instituição de saúde portuguesa.

Controlo de Acessos

- Cada membro da instituição deve aceder à infraestrutura através de credenciais de acesso, de modo a não comprometer a segurança e os dados da instituição;
- Devem ser atribuídas a cada membro da instituição credenciais de acesso, de acordo com a função do colaborador na instituição, seguindo normas reguladas pela mesma. Estas credenciais devem ser únicas;
- Para cada membro deve ser especificado o seu nível de acessos e permissões na infraestrutura tendo em conta a sua função, tendo apenas acessos para o cargo que desempenha, excetuando alguns casos;
- Os acessos e permissões de cada membro devem ser revistos em intervalos de tempo definidos pela instituição, de modo a restringir acessos não autorizados;
- O processo de atribuição, revisão e revogação de acessos deve ser automático, após aprovação de um membro superior da instituição;
- A infraestrutura deve ser capaz de monitorizar e registar toda a atividade dos funcionários relacionada com gestão dos dados, com especial atenção a dados sensíveis.

Classificação de Dados

- Todos os dados relativos à instituição devem ser categorizados em níveis de classificação de acordo com a sua sensibilidade, sendo o nível inicial relativo a dados de divulgação externa, e os seguintes níveis de cariz restrito ou confidencial;
- Os dados em cada nível de classificação devem ser armazenados e tratados de maneira diferente, consoante a sua sensibilidade;
- Os dados devem ser alvo de períodos de retenção e sujeitos a apagamento de forma distinta, devendo a instituição definir um período de retenção adequado a cada nível de classificação e proceder ao apagamento de dados seguindo um conjunto de etapas que assegure que esses dados são evidentemente apagados.

Encriptação de Dados

- Para dados sensíveis, deve ser definido pela instituição um método de encriptação tanto para dados armazenados como para dados em tráfego de rede;
- As chaves de encriptação e desencriptação dos dados devem ser restritas a certos membros da chefia da instituição, e devem ser seguidas boas práticas para a sua confidencialidade;
- Para canais de comunicação, troca de emails ou outros meios onde haja envio e receção de informações, devem ser especificados e implementados protocolos de comunicação seguros;
- Cada membro da instituição deve utilizar no seu computador pessoal uma VPN disponibilizada pela instituição.

Resposta a Incidentes

- A instituição deve criar uma equipa de resposta a incidentes e instaurar um plano de resposta a incidentes que explique que medidas tomar face a um incidente ou uma fuga de dados;
- A instituição deve atribuir papéis e responsabilidades aos membros da equipa de resposta a incidentes;
- Com foco na prevenção, devem ser estabelecidos procedimentos para documentar incidentes previamente ocorridos, e após um incidente conduzida uma análise com vista a verificar possíveis vetores de vulnerabilidade.

Backups e Restauros

- Todos os membros da instituição devem possuir na rede uma pasta pessoal para armazenamento de informação pessoal, acessível apenas para aquele membro;
- A instituição deve definir períodos específicos para backups periódicos da informação a que cada membro está sujeito, assim como períodos de retenção de dados;
- Regularmente devem ser executados processos de backup e restauro de dados, de modo a assegurar que os mesmos funcionam e não apresentam falhas;
- Em caso de falha de algum sistema da instituição, deve ser implementada redundância da informação e medidas de recuperação de desastres para diminuir o tempo de inatividade da instituição.

Security Awareness e Formações

- Os membros da instituição devem ter sessões obrigatórias e sessões regulares de consciencialização para a segurança informática;
- De modo a reconhecer ataques de engenharia social, ataques de phishing ou outro tipo de ameaças à segurança, cada membro da instituição deve ser educado e sensibilizado para tal;
- Deve ser promovida uma cultura institucional que determine boas práticas de gestão da informação.

Gestão de Riscos Externos

- A instituição deve estabelecer guidelines para avaliação e gestão de riscos associados a terceiros;
- Distribuidores de software ou fornecedores de serviços à instituição devem cumprir padrões de segurança e preencher requisitos de cumprimentos legais;
- A relação com entidades externas deve ser regularmente acompanhada e monitorizada de modo a mitigar potenciais vulnerabilidades.

Conformidade Regulatória

- As guidelines e normas internas à instituição devem estar em conformidade com o Regulamento Geral de Proteção de Dados e a Resolução 41/2018 do Conselho de Ministros;
- Os membros superiores da instituição devem estar informados e atualizados sobre novas normas legislativas de segurança ou eventuais alterações e atualizar as políticas internas de acordo com essas mudanças.

Standards

Definição: São ações ou regras que suportam e estão em conformidade com as políticas. Devem dar mais sentido às políticas e incluir uma ou mais especificações aceites de hardware ou software.

Autenticação e Autorização

Deve ser seguido o requisito técnico presente no anexo da resolução 41_2018 do conselho de ministros 'Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações'.

É recomendado o uso de *Transport Layer Security* (TLS) na sua versão mais recente, ou o uso de palavra-passe, em combinação com outro fator (autenticação dois fatores - 2FA), como por exemplo:

- Palavra -passe + SMS Token;
- Palavra -passe + Smartcard;
- Palavra -passe + Biometria;
- Palavra -passe + padrão gráfico;
- Palavra -passe + Cartão de coordenadas;
- Palavra -passe + código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR Code.

Como mecanismo de proteção e segurança da informação a nível da App, recomenda-se o uso de Token. Se possível, devem ser usados certificados através de API, não sendo desta forma necessário o uso de palavras-passe.

Controlo de Acessos

Devem ser seguidos os seguintes requisitos técnicos presentes no anexo da resolução 41_2018 do conselho de ministros:

- 'Arquitetura de segurança das redes e sistemas de informação', relativamente a autenticação, credenciais de início de sessão, Hash, password e padrão de autenticação;
- 'Atribuição de direitos de acesso e privilégio de forma restrita e controlada', relativamente a registos de acessos, alterações e remoções (logs);
- 'Restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil)', relativamente ao tipo de perfil atribuído a cada membro da instituição – princípio dos privilégios mínimos.

Defesa de Perímetro

O perímetro de rede é considerado uma primeira linha de defesa contra ameaças externas. De modo a proteger a infraestrutura da instituição, deve ser configurada adequadamente uma Firewall, permitindo fazer a filtragem do tráfego de acordo com as necessidades da instituição e evitando a exposição a protocolos de comunicação e fluxos desnecessários ou perigosos.

Deve ser seguido o requisito técnico presente no anexo da resolução 41_2018 do conselho de ministros 'Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional'.

Práticas de Desenvolvimento Seguro

Deve ser seguido o requisito técnico presente no anexo da resolução 41_2018 do conselho de ministros 'As aplicações cliente (exemplo, Android, IOS, WEB) devem ser desenvolvidas adotando práticas de desenvolvimento seguro'.

As aplicações cliente devem ser desenvolvidas seguindo boas práticas de desenvolvimento, isto é, utilizar sessões seguras com protocolo de segurança, recomendando o uso da versão mais recente de *Transport Layer Security* (TLS). Devem também não guardar informação pessoal no *browser*, memória ou disco, para além do tempo da sessão e apenas na medida do necessário, assim como embeber palavras-passe no código.

Princípio dos Privilégios Mínimos

Cada utilizador da framework apenas deve possuir privilégios que correspondam à função que desempenha na instituição:

- Cada pessoa pode aceder ao seu boletim de vacinas;
- Cada profissional de saúde pode apenas aceder ao nome e data de nascimento (para validação) de uma pessoa, assim como ao boletim de vacinas da pessoa para consultar o tipo e data de vacinas tomadas;
- Funcionários em cargos superiores podem aceder ao número de pessoas com uma, duas ou três doses, e o número total de vacinas usadas;
- Informações providenciadas por organizações de saúde europeias e OMS's vão estar disponíveis, ao aceder a uma página web pública com credenciais específicas.

Proteção dos Dados Contra Modificações Não Autorizadas, Perdas, Furtos e Divulgação Não Autorizada

Deve ser seguido o requisito técnico presente no anexo da resolução 41_2018 do conselho de ministros 'Devem ser definidas políticas que garantam a segurança dos dados pessoais, em alinhamento com a estratégia superiormente definida para a segurança do tratamento de dados pessoais', assim como o artigo 5º 'Principles relating to processing of personal data' presente no capítulo 2º 'Principles' do regulamento geral de proteção de dados.

As políticas que garantam a segurança do tratamento de dados pessoais devem abranger a priorização e classificação dos dados de acordo com os critérios de sensibilidade e criticidade predefinidos, a criação, modificação, transmissão, recolha, destruição, armazenamento e a pesquisa de dados.

Redundância e Disponibilidade dos Sistemas de Armazenamento

Deve ser seguido o requisito técnico presente no anexo da resolução 41_2018 do conselho de ministros 'Os sistemas de armazenamento devem garantir redundância e disponibilidade, não devendo existir nenhum «single point of failure»'.

A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.

Respeito pelos Direitos do Titular dos Dados

Deve ser seguida a norma presente no anexo da resolução 41_2018 do conselho de ministros 'As redes e sistemas de informação devem possuir as funcionalidades necessárias ao respeito pelos direitos do titular dos dados', assim como os artigos 16º, 17º, 18º, 19º e 20º presentes na secção 3 'Rectification and erasure' do regulamento geral de proteção de dados.

Os sistemas devem estar capacitados para classificar, priorizar, pesquisar, editar e apagar os dados pessoais, e devem possuir os controlos necessários que permitam a identificação, autenticação, acesso e validação dos dados pessoais armazenados.

Segurança dos Dados Pessoais

Deve ser seguida a norma presente no anexo da resolução 41_2018 do conselho de ministros "Arquitetura de segurança das redes e sistemas de informação", assim como os artigos 32º, 33º e 34º presentes na secção 2 'Security of personal data' do regulamento geral de proteção de dados.

Devem ser definidas políticas que garantam a segurança dos dados pessoais, em alinhamento com a estratégia superiormente definida para a segurança do tratamento de dados pessoais.

Uso de Palavras-passe

Deve ser seguido o requisito técnico presente no anexo da resolução 41_2018 do conselho de ministros “Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações”.

Sempre que aplicável, a palavra -passe deve ter no mínimo 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa. A sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : “ ; ‘ < > ? , . /).

Guidelines

Definição: Recomendações ou instruções administrativas concebidas para atingir os objetivos das políticas. Podem mudar frequentemente de acordo com o ambiente e deve ser revistas regularmente.

Segurança Lógica

- Cada membro da instituição deve abster-se de partilhar as suas credenciais de acesso com outro;
- Cada membro da instituição deve suspender o seu dispositivo pessoal (computador ou telemóvel) quando se afasta do mesmo por um período de tempo elevado;
- As credenciais de acesso do membro devem ser atualizadas de 4 em 4 meses, seguindo as normas de criação de palavras-passe. Caso o membro não cumpra esta atualização antes do tempo limite, as suas permissões são revogadas.
- Os direitos de acesso de cada membro da instituição devem ser revistos mensalmente, de modo a restringir acessos não autorizados;
- Para se autenticar na framework, cada utilizador deve usar palavra-passe em conjunto com token;
- Sempre que o utilizador for forçado a alterar a sua palavra-passe, a nova palavra-passe não deve ser semelhante nem incluir elementos de palavras-passe antigas;
- Caso o utilizador insira incorretamente as suas credenciais de acesso 3 vezes, este fica imediatamente bloqueado de aceder à framework, tendo de se deslocar ao suporte técnico para recuperar os acessos;
- Para aceder ao servidor web e ao servidor de ficheiros, cada utilizador deve usar palavra-passe juntamente com autenticação 2 fatores;
- Os computadores pessoais entregues pela instituição aos membros devem ter firewall, VPN e pasta de rede configurados, entradas usb configuradas para bloqueio de dispositivos de armazenamento externo, comandos cmd e aplicações limitadas e alguns domínios web bloqueados;
- Os computadores pessoais entregues pela instituição aos membros devem ter a versão mais recente do sistema operativo e das aplicações permitidas, e as atualizações de software devem ser forçadas sempre que estiverem disponíveis;
- O tráfego de rede deve ser monitorizado diariamente de modo a detetar possíveis vulnerabilidades no sistema;
- Cada servidor da infraestrutura deve ter a sua própria firewall, de modo a fazer uma separação lógica dos componentes da rede e garantir disponibilidade e confiabilidade;
- Deve ser feito um controlo de dados da firewall para detetar intrusões no sistema;
- A configuração da firewall deve bloquear todo o tráfego não permitido, aplicando a regra de ‘deny by default’;

- Para cada utilizador deve ser feito um registo de atividade mensal em forma de logs sobre todas as ações realizadas pelo mesmo a nível de acessos e tentativas falhadas, assim como a navegação web e acesso ao servidor de ficheiros. De modo a associar as ações ao utilizador, o registo de atividade deve conter o endereço IP de origem, endereço IP de destino, hash do IP de origem, data e hora do acesso, e a ação efetuada (url do website ou a aplicação acedida). Para assegurar os princípios CID, os registos devem ser classificados com o nível 'Confidencial', assinados digitalmente por um membro da chefia da instituição e armazenados no servidor de ficheiros, acessíveis através de credenciais específicas;
- Todos os email provenientes de remetentes internos e externos à instituição devem ser analisados antes de qualquer ação. Anexos e links não devem ser abertos se o remetente for externo à instituição. O email institucional não deve ser usado para fins fora do contexto laboral (criação de redes sociais, newsletters de revistas, discussão em fóruns online, etc.);
- Os membros da instituição não devem aceder a websites com as seguintes características:
    - Redes sociais;
    - Websites de jogos e apostas;
    - Pornografia;
    - Plataformas de streaming de vídeo e música;
    - Comércio eletrónico.
- Toda a informação armazenada e em tráfego de rede deve ser criptografada. Deve ser usado o AES como algoritmo de criptografia e o SHA-256 como hash de encriptação;
  O Advanced Encryption Standard (AES) é o algoritmo padrão usado pelo governo dos EUA e várias organizações. Embora seja altamente eficiente no formato de 128 bits, o AES também usa chaves de 192 e 256 bits para fins de criptografia pesada. O SHA-256 é uma das funções hash mais robustas atualmente, e serve como bom complemento ao AES;
- Sempre que um utilizador aceda remotamente ao servidor web, a VPN é usada como mecanismo de cifra ponto a ponto;
- As chaves de encriptação e desencriptação devem estar armazenadas no servidor de dados, acedidas através de certos membros da instituição com credenciais específicas;
- Os backups efetuados devem estar armazenados no servidor de ficheiros da instituição, mas também num edifício da mesma organização geograficamente mais distante, de maneira a garantir redundância e disponibilidade.

Segurança Física

- Apenas determinados membros da instituição têm acesso à sala de servidores da instituição;
- A sala de servidores deve estar devidamente refrigerada de modo a evitar sobreaquecimento dos componentes e eventual dano;
- A sala de servidores apenas é acessível via cartão magnético;
- Os cartões magnéticos para acesso à sala de servidores não devem ser levados com nenhum membro para fora da instituição;
- Na sala de servidores deve estar presente uma UPS (Unlimited Power Supply) que permita alimentar os servidores durante alguns minutos, em caso de corte de energia na instituição;
- Deve existir na instituição um gerador de emergência em complemento com a UPS;
- Os membros da instituição não devem utilizar dispositivos de armazenamento externo (Pen USB, Disco Externo, etc.) para funções laborais, devendo para isso usar o servidor de ficheiros.

Procedimentos

Definição: Instruções sobre como executar uma certa tarefa ou atividade. De seguida estão descritos procedimentos gerais que são relevantes para a instituição.

Tratamento das credenciais de um funcionário

As credenciais de cada funcionário deverão ser únicas e intransmissíveis. As credenciais designadas ao funcionário deverão ser entregues presencialmente e não deverão ser vistas por outro funcionário. O funcionário deverá será alertado que a palavra-passe deverá ser alterada na primeira vez que este se autentique pela primeira vez. O funcionário deverá confirmar que recebeu as credenciais. A palavra-passe deverá corresponder aos requisitos mínimos de segurança como tamanho, uso de caracteres especiais e combinação de números com letras.

Entrega dos dispositivos ao funcionário

O dispositivo que é fornecido ao funcionário deverá já ter executada pelo departamento de IT a encriptação de dados, instalação da firewall e do antivírus. O funcionário deverá receber normas de como proteger o seu dispositivo.

Reativação de conta de utilizador

Se for observado que uma conta não apresenta atividade durante pelo menos 3 meses, esta será desativada. Se após os próximos 3 meses não houver alterações no mesmo estado, esta será eliminada. A reativação da conta apenas será permitida por parte das pessoas de TI responsáveis.

Revisão de privilégios de utilizadores

Os privilégios de utilizadores devem ser baseados no princípio dos privilégios mínimos. Para a confirmação de que os utilizadores têm atribuídos os privilégios, corretos deve ser efetuada trimestralmente uma verificação dos mesmos. Se um utilizador quiser aceder a algo que não tem privilégio, deverá efetuar um pedido para a revisão do seu caso de forma a poder ser aprovada a sua alteração, e com isso deve-se proceder às alterações necessárias.

Monitorização e registo de atividades

As atividades de acesso e registos devem ser registados em logs, e estes devem incluir atividades temporais (como data e hora), utilizador, recursos a que acedeu e ações que realizou. Os logs deverão ser protegidos de forma a não haver exclusão ou alteração dos mesmos. Deve existir um sistema que permita monitorar violações de segurança, bem como comportamentos estranhos e atividades estranhas. Este sistema deverá alertar a equipa de segurança de potenciais ameaças.

Vulnerabilidades Web

Quando for detetada uma vulnerabilidade, esta deve ser tratada o mais rapidamente possível de forma a diminuir o tempo da mesma poder ser explorada. Após a correção, a aplicação deverá ser submetida a novos testes para verificar que a vulnerabilidade já não se encontra presente.

Deteção de atividade suspeita

De forma a verificar possível atividade suspeita, os logs devem ser analisados regularmente. Deverão estar atentos a possíveis evidências de:

- Acessos não autorizados ao sistema de ficheiros;
- Acessos não autorizados ao servidor web;
- Acessos não autorizados à base de dados;
- Comportamento suspeito como por exemplo SQL Injection, XSS, upload de ficheiros.

Como os logs poderão conter muita informação desnecessária para a análise, é recomendado que haja uma filtração, para melhor visualização.

Sitografia

1. https://www.cncs.gov.pt/docs/cncs-roteiro-capacidades-minimas-ciberseguranca.pdf
2. https://www.enisa.europa.eu/topics/cybersecurity-policy
3. https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
4. https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future
5. https://www.movable-type.co.uk/scripts/sha256.html
6. https://www.techtarget.com/searchsecurity/tip/How-many-firewalls-do-you-need
7. https://owasp.org/www-pdf-archive/Effective_Software_Security_Management.pdf
8. https://www.convergepoint.com/policy-management-software/policy-procedure-best-practices/5-steps-ensure-compliance-policies-procedures/
9. https://eur-lex.europa.eu/eli/reg/2016/679/oj
10. https://dre.pt/application/conteudo/114937034
11. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf