GUIA DE SEGURANÇA NO TELETRABALHO

SAIBA COMO PROTEGER A SUA EMPRESA REMOTAMENTE EM 6 PASSOS.

MOVING BUSINESS FORWARD

www.eurotux.com

eurotux

Índice

Introdução..... 1

Importância de proteger a informação..... 2

Tipos de ameaças à segurança da informação.....3

Boas-práticas de cibersegurança em 6 passos..... 4

1. Utilize software atualizado e de confiança.....5

2. Defina uma password longa, forte e fácil de memorizar..... 6

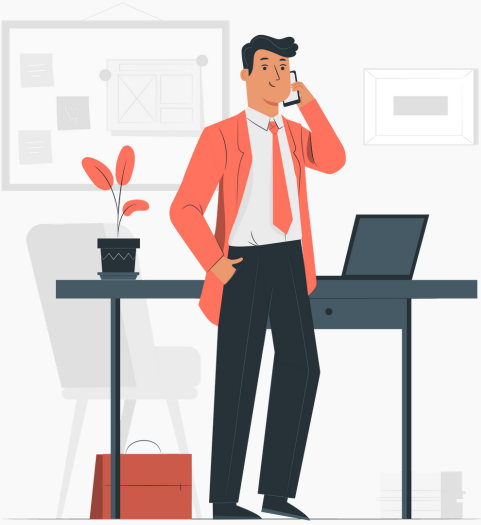
3. Ative a autenticação em duas etapas..... 11

4. Esteja atento a sinais de burla..... 14

5. Conecte-se sempre à rede privada da sua organização..... 19

6. Tenha um ambiente de colaboração remota seguro..... 20

Conclusão..... 23



Introdução

A pandemia provocada pela Covid-19 intensificou e generalizou uma prática permitida apenas em algumas empresas mais tecnológicas: o teletrabalho. O abrupto crescimento de postos em teletrabalho trouxe novas preocupações e desafios para a cibersegurança das organizações.

Uma das principais mudanças prende-se com a responsabilidade sobre a segurança da informação, que antes era assegurada sobretudo pelos especialistas informáticos e de repente passou a ser também função do próprio colaborador que trabalha a partir de casa em condições que a empresa não controla.

Antes da pandemia, a maioria dos colaboradores trabalhava nas instalações das empresas, e por isso, a prioridade dos administradores de sistemas era a proteção das redes internas e não tanto dos postos de trabalho (*endpoints*). Contudo, a realidade mudou e a informação das empresas, nomeadamente emails, contratos e listagens, circulam pelos dispositivos e redes pessoais dos seus colaboradores com níveis de proteção bastante baixos. Por este motivo, torna-se essencial informar os colaboradores dos perigos e consequências dos ataques informáticos e ainda sobre as boas práticas relativas à segurança da informação.

Este guia pretende ajudar as empresas ou instituições a transmitirem aos seus colaboradores as boas práticas a seguir, para em conjunto se protegerem contra os ataques informáticos e o roubo de informação. Através de uma linguagem simples e didática, são apresentados boas práticas de segurança em 6 passos.. Por fim, a Eurotux partilha ainda algumas das suas opções relativamente a ferramentas a utilizar no contexto do trabalho remoto.

Importância de proteger a informação

É fundamental proteger a informação da empresa onde trabalha, porque quando os dados são roubados, é necessário pagar valores muito elevados para os recuperar, isto quando não caem diretamente nas mãos de concorrentes ou são divulgados na Internet.

Quando alguém acede indevidamente aos dados de uma empresa, pode acontecer o seguinte:

- Faz uma cópia da informação e expõe na Internet;
- Faz uma cópia da informação e vende a concorrentes;
- Torna os dados ilegíveis (encriptados) e pede um resgate;
- Apaga os dados de forma irrecuperável.

Já imaginou se a sua empresa perdesse os contratos, planos, emails entre outras informações importantes, só porque abriu um email indevidamente?

Por outro lado, com o Regulamento Geral sobre a Proteção de Dados (RGPD) que entrou em vigor em 2018, um incidente de segurança que exponha dados pessoais pode ter consequências irreversíveis para as empresas independentemente da sua dimensão. A responsabilidade sobre os dados recolhidos aumentou, e portanto devem ser muito bem protegidos.

É importante ter presente que os ataques informáticos são cada vez mais frequentes, sofisticados e motivados por um bem muito valioso: a informação.

Tipos de Ameaças à Segurança da Informação

Quando ameaçada, a informação pode perder qualquer uma das suas 3 principais características:

- **Perda da Confidencialidade** - quebra do sigilo, alguém acede a uma informação confidencial como os emails enviados por toda a empresa;
- **Perda da Integridade** - quando alguém altera a informação sem ter autorização para tal;
- **Perda da Disponibilidade** - a informação é movida ou eliminada e por isso deixa de estar acessível quando algum colaborador precisa dela (tal como acontece nos ataques de *ransomware*).

As ameaças podem partir de agentes maliciosos externos, por meio de *malware* ("vírus") presentes em ficheiros corrompidos, recebidos por algum canal de comunicação (email, SMS, WhatsApp e *downloads*); ou ainda por *social engineering* (tema do Passo 4), método que muitas vezes é utilizado como parte dum plano maior para roubar informações e aceder a algum sistema crítico.

Um tipo frequente de ameaça às empresas é o *ransomware*: ficheiro malicioso que entra no computador da pessoa, geralmente por email ou chat, e que altera a informação de forma a ficar ilegível (encriptada). A informação deixa assim de estar disponível, e o responsável pelo ataque pede elevados valores em **criptomoeda** como resgate.

Exemplo: a Bitcoin

Nestas circunstâncias as organizações que tenham um bom sistema de Backups (cópias de segurança dos dados) estão salvaguardadas relativamente à perda dos dados, embora se mantenha o risco de verem os seus dados expostos na Internet.

Boas-práticas de cibersegurança em 6 passos

Este guia vai dar-lhe a conhecer algumas boas práticas para reduzir a probabilidade de ser vítima de ataque informático, e deixá-lo(a) mais alerta quanto a possíveis vulnerabilidades habitualmente exploradas pelos cibercriminosos (*hackers*). Segue a lista dos 6 passos:

1. Utilize *software* atualizado e de confiança
2. Defina uma *password* longa, forte e fácil de memorizar
3. Ative a autenticação em duas etapas
4. Esteja atento a sinais de burla
5. Conecte-se sempre à rede privada da sua organização
6. Utilize programas de colaboração remota seguros

1. Utilize *software* atualizado e de confiança

PARA AS EMPRESAS

O primeiro passo para proteger a informação da sua empresa é assegurar que os sistemas operativos e o *software* utilizados são adequados e necessários às funções dos colaboradores. Estes devem estar devidamente atualizados e com os patches de segurança em dia.

Existem diversas soluções que permitem detetar vulnerabilidades, bloquear e impedir mensagens, emails ou ficheiros maliciosos (*malware*), assim como reparar os seus danos, e ainda identificar possíveis eventos futuros.

PARA OS COLABORADORES EM TELETRABALHO

Além de ter o *software* adequado instalado no seu computador, é necessário que o mesmo esteja atualizado, pois desta forma os problemas de segurança que poderiam ser exploradas por *hackers* serão corrigidos.

Alerte a sua empresa sempre que lhe surgir alguma mensagem a indicar que o *software* deve ser atualizado.

5 ALIADOS DA EUROTUX PARA A CIBERSEGURANÇA

1. **Proteção de Endpoint:** Intercept X Endpoint - Um poderoso aliado contra *Malware*, *Ransomware*, *Exploits* e Vírus.
2. **Anti-Phishing:** Sophos Phish Threat - Simulações de ataque de *Phishing* e formação para os colaboradores.
3. **Proteção de Rede:** Sophos XG Firewall - *Firewall* com uma arquitetura que proporciona elevados níveis de proteção, enorme visibilidade da sua rede, utilizadores e aplicações, com um invejável desempenho.
4. **Criptografia:** Sophos Central Device Encription - Integra com as soluções nativas Windows (BitDefender) e macOS (FileVault) e realiza a ativação e gestão da cifragem dos discos rígidos dos computadores dos colaboradores.
5. **Backup:** Veeam - Solução de backup que abrange diferentes estratégias. É também a tecnologia base da solução as-a-Service Eurotux eBackup, para backups off-site.

2. Defina uma *password* longa, forte e fácil de se memorizar

ERROS COMUNS

Deve evitar ao máximo utilizar *passwords* como as descritas a seguir.

Descrição	Exemplos
Dado pessoal, público e/ou facilmente obtido.	antoniomoreira (nome) 12021980 (data de nascimento) sporting (clube de futebol)
Sequências do teclado	qwerty 123456789
Sequências numéricas e números conhecidos	123456789 112 123123
Utilizar as passwords que os sites sugerem (default *passwords*) - pois há inúmeras listas com estas passwords na Internet;	admin
Apenas palavras do dicionário	vermelho pipoca
Palavras seguidas de um número	vermelho1375 pipoca982
Palavras em que as letras são substituídas por números (leet) - pois há formas de permutar palavras do dicionário com estas variações conhecidas	p4ssw0rd 1nv3rn0
Palavras repetidas - pois são fáceis de serem descobertas.	pipocapipoca

Por último, não utilize as mesmas passwords em diferentes serviços, como por exemplo no email, nas redes sociais ou no *homebanking*. Uma vez comprometidas as suas credenciais para algum serviço, é muito provável que os atacantes consigam aceder aos restantes sites ou serviços onde utiliza essa mesma password.

Dicas para definir uma boa *password*

As boas práticas atuais definem que uma password deve ter 12 caracteres, e de preferência respeitar a regra seguinte:

- Alguma letra maiúscula (ABCDE...);
- Alguma letra minúscula (abcde...);
- Algum número (1234...);
- Algum caractere especial (!"#$%&...).

Uma ótima forma de definir uma boa *password* é através da criação de frases mnemónicas (auxiliares de memória), a partir de trechos de música, livros, poemas ou algo que goste. Seguem alguns exemplos:

Frase	Password	Ínspiração
"Três vezes do leme as mãos ergueu, Três vezes ao leme as reprendeu,"	3xdLaME,3xaLaR	Citação: O Monstrengo – Fernando Pessoa
Eu adoro remar no rio Douro!	eA2RnrD!	Pessoal: Desporto/Hobby
"to be a rock and not to roll"	2BaR&n2R	Música: Stairway to Heaven - Led Zeppelin

Proteja-se do *Brute Force* com uma maior entropia

O primeiro passo para definir uma boa *password* é perceber quais são os métodos utilizados pelos *hackers* para as descobrir. Entre eles, o ***brute force*** é o mais comum, e consiste num *software* que funciona por tentativa e erro, de inúmeras combinações e *passwords* conhecidas diferentes, até encontrar a sua.

Para resistir a este método, é importante perceber o conceito de bits de **entropia**, criado para medir o quão forte é uma *password*.

- Uma *password* conhecida tem 0 bits de entropia, ou seja, é facilmente descoberta;
- Uma *password* que requeira duas tentativas para acertar, tem 1 bit de entropia.
- Uma *password* com "n" bits de entropia, requer 2^n tentativas para ser descoberta.

Utilizar as **dicas para definir uma boa *password***, apresentadas anteriormente, aumenta a entropia e torna a password mais difícil de ser descoberta.

Dictionary Attacks

Muitas *passwords* podem ser facilmente descobertas através dos conhecidos "*dictionary attacks*". Este tipo de ataque tenta as combinações presentes numa base de dados, como um dicionário, até encontrar a *password* em questão.

Para diminuir a probabilidade da sua *password* ser descoberta num *dictionary attack*, pode optar por combinar mais do que uma *password* (*passphrase*). Quanto mais aleatória for, melhor. Contudo, é sabido que os humanos têm dificuldade em criar combinações que sejam realmente aleatórias. E para colmatar esta limitação têm surgido ao longo dos anos vários métodos como o descrito a seguir: método *Diceware*.

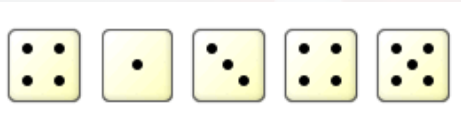
O Método *Diceware*

O método *diceware* consiste na utilização de um dado (gerador de números aleatórios), para obter números de 5 dígitos, que depois são substituídos pela palavra correspondente numa lista. O seu objetivo é criar frases de 5 ou mais palavras aleatórias, de forma *offline*, para maior segurança. Cada palavra adiciona 12.9 bits de entropia à *passphrase*.

Passo-a-passo:

- **Jogue o dado 5 vezes e anote os números;**

  Ex.:



- **Encontre a palavra correspondente na lista de palavras;**

  Ex.:

41343	lockout
41344	locucao
41345	lodo
41346	log
41351	logica

- **Repita o mesmo por 5 vezes no mínimo, e crie uma frase;**

  Ex.: lodo carro baleia memória vampiro

Pronto! Agora tem uma *passphrase* difícil de ser quebrada pelos métodos tradicionais, com muitos *bits* de entropia. Uma vez que ela faz sentido para você, ela será facilmente memorizada.

Guardar as *Passwords*

Anotar cada nova *password* no papel, criada para uma infinidade de serviços que utilizamos todos os dias, não é a forma mais prática de guardar as suas credenciais.

Hoje existem vários programas que permitem gerir passwords e facilitam o trabalho de as criar e memorizar. Mas ainda assim é necessário definir uma *password* muito forte para guardar todas as suas outras.

Gestores de password recomendados:

Lastpass - conhecido por ter o melhor plano *freemium* entre os gestores de *passwords*, pois não há limite de dispositivos ou de *passwords*. Além disso há a possibilidade de integração com autenticadores, caso pretenda utilizar a autenticação em duas etapas. As *passwords* criptografadas ficam armazenadas online, na cloud.

KeePass - opção offline open-source totalmente gratuita. Utiliza os melhores algoritmos de criptografia conhecidos.

Teampass - Um gerenciador de *passwords open-source* e colaborativo, que permite a partilha de credenciais. Utiliza diversos níveis de encriptação. Além disso os dados ficam armazenados no servidor web da própria organização e é facilmente customizável.

3. Ative a autenticação em duas etapas

Como visto no tópico anterior, as *passwords* podem ser facilmente comprometidas através de métodos como *Brute Force* e *Dictionary Attacks*.

É necessário portanto estabelecer novas medidas de segurança, e o *multi-factor authentication* (MFA) é uma excelente ferramenta complementar.

O poder do *multi-factor authentication* (MFA)

O MFA é um método de autenticação no qual o acesso só é garantido com a apresentação de duas ou mais provas (fatores) de que a pessoa que está a aceder é efetivamente quem diz ser.

Tipos de fatores de autenticação

- **Algo que a pessoa possui (fator de posse):** token, cartão, chave, telemóvel, etc.
- **Algo que a pessoa sabe (fator de conhecimento):** PIN, *password*, pergunta de segurança sobre uma informação pessoal, etc.
- **Algo único na pessoa (fator inerente):** impressão digital, íris, velocidade de digitação, etc.
- **Relativo a algum lugar onde a pessoa está (fator baseado em localização):** conexão a uma rede específica ou localização de GPS.

Estes quatro fatores compõem os pilares da autenticação, no entanto alguns deles podem ser facilmente ultrapassados, como as perguntas de segurança (fator de conhecimento), que são conhecidas por determinadas pessoas ou podem ser investigadas através de **redes sociais**.

> Devemos ser cuidadosos com a informação que expomos na Internet (mesmo que as contas sejam privadas). Há muitas formas de se aceder aos dados. A partir do momento em que esteja na Internet, há pessoas que vão conseguir aceder-lhe.

A *password* é o tipo de fator de conhecimento mais utilizado na autenticação em 2 etapas (*two-factor authentication* - 2FA), mas geralmente é o elo mais fraco. Por isso é pedido um outro fator adicional como o de posse.

Os fatores de posse são uma das formas mais antigas de autenticação. No mundo digital, os fatores de posse podem ser *tokens* desconectados que geram códigos aleatórios, *tokens* de *hardware*, como a Yubico Yubikey e a Google Titan Key, ou *tokens* de *software*, como as apps OTP (*One Time Password*) de autenticação nomeadamente Free OTP, Microsoft Authenticator e Google Authenticator.

Os telemóveis também são amplamente utilizados como fator de posse, com autenticação *push* ou via SMS, mas ainda há a possibilidade de serem clonados e usados indevidamente. Por isso há a crescente utilização de um terceiro fator (3FA), a partir de leituras biométricas (impressão digital, reconhecimento facial, de voz ou íris, da dinâmica de digitação), ou mesmo da localização do utilizador.

Qual tipo de MFA é aconselhável para a minha organização?

Para obter um maior grau de segurança, a Eurotux aconselha que sempre que possível utilize no mínimo a 2FA para permitir o acesso remoto à informação crítica para a empresa. Isto pode ser possível quando seja necessária a introdução de uma *password* e outro fator de autenticação, que pode ser via SMS, *Token*, OTP ou localização.

De forma a garantir a segurança máxima, a 4FA é recomendada. Neste caso, por exemplo, poderiam ser necessárias *passphrase* (conhecimento), *hardware token* (posse), localização e impressão digital (inerente) para a concessão do acesso.

Cada organização deverá decidir, dependendo dos sistemas e/ou sensibilidade da informação que protegem, qual o número e tipo de factores de autenticação a utilizar.

Estas barreiras contra o acesso indevido à informação e plataformas críticas das organizações não são totalmente à prova de falha. Os utilizadores mesmo assim estão suscetíveis a ataques de *phishing* e outras técnicas de *social engineering*, tema que será abordado a seguir.

4. Esteja atento aos sinais de burla

As ações e comportamento dos colaboradores são um fator determinante para a segurança da informação das organizações. A pandemia causou uma intensificação de ataques de *ransomware* e *phishing*, além de uma série de *scams* que utilizavam como tema a COVID-19. Segundo um estudo da Gallagher de 2020, cerca de 60% das falhas de segurança são causadas por erro humano.

Muitos destes ataques, como o incidente envolvendo comprometimento das ferramentas administrativas do Twitter de Julho de 2020, iniciaram-se a partir do *social engineering*, e poderiam ter sido evitados com uma maior educação dos colaboradores, ou a implementação da forte cultura de segurança da informação.

O que é *social engineering*?

Social engineering é a manipulação psicológica com o objetivo de obter informações confidenciais ou realizar determinadas ações, geralmente utilizada por cibercriminosos para obter acesso ou iniciar um ataque.

As vulnerabilidades exploradas neste caso são as distorções de julgamento das vítimas, que acabam por tomar ações precipitadas, sem verificar a identidade de quem solicita ou da autenticidade do pedido.

Num ataque de *vishing* (phishing por telefone) por exemplo, o criminoso pode apresentar como algum colaborador do suporte técnico e pedir, com senso de urgência, que se insira algum comando no seu PC. Neste caso o a pressão faz com que a vítima a tome uma ação precipitada, sem verificar as credenciais do suposto colaborador, estando vulnerável ao roubo de dados ou invasão do sistema informático.

Quais são os principais tipos de *social engineering*?

- *Vishing* - também conhecido como voice *phishing* (por telefone), é utilizado para obter informações como emails de colaboradores e credenciais, ou como forma de reconhecimento da superfície de ataque da organização;

- *Phishing* - técnica para obtenção de informações credenciais e de cartão de crédito, geralmente enviada por email, (em nome de um banco ou outro serviço). Solicita que seja feito o login numa página réplica falsa, que rouba os dados inseridos nela.

- *Smishing* - é quando o mesmo golpe é realizado via SMS;

- *Impersonation* - é quando o criminoso finge ser outra pessoa para ter acesso à determinado sistema informático, prédio ou informação.

No caso do *spear phishing*, os emails podem ser altamente personalizados e enviados para poucas pessoas selecionadas, enquanto no phishing em massa, são enviados sem personalização para o maior número de pessoas possível.

Como detetar ataques de Phishing?

De acordo com a Sophos, 41% das organizações experimentam ataques de *phishing* diariamente, e mais de três quartos (77%) experimentam um ataque de *phishing* pelo menos uma vez por mês. Por isso é muito importante saber detetar estes ataques.

Esteja atento a sinais como:

- Erros ortográficos e má gramática;
- Senso de urgência, por exemplo faturas vencidas e/ou interrupção de serviços;
- Promessas de recompensa em dinheiro, por exemplo;
- Consequências graves caso não faça o que pedem;
- Palavras fortes e enervantes (como "A sua conta foi violada!");
- Saudações genéricas (Ex.: “Caro cliente”); e
- Solicitação de dados e informações pessoais e organizacionais sensíveis.

Além disso, é possível que os criminosos utilizem alguma informação pessoal obtida através das redes sociais, para personalizar o email e parecer convincente.

O *spear phishing*, tendo uma mensagem mais personalizada, tende a ser mais difícil de se identificar. Estes, geralmente são direcionados para executivos C-level (CEO, CTO CFO), uma vez que são estes que detêm informação crítica.

A melhor forma de prevenção contra o *phishing* é através de simulações e formações feitas pelos administradores de sistema, de forma que os colaboradores aprendam a identificar possíveis ataques. Além disso a proteção dentro das plataformas de email e *endpoints* é recomendada.

Esteja atento a possíveis ataques de *pretexting*

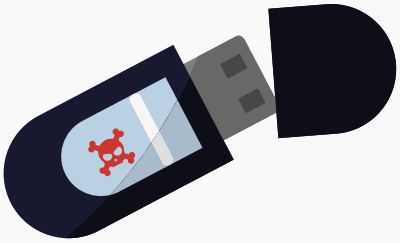
Os ataques de *pretexting* (pretexto) ocorrem quando os criminosos criam algum cenário fictício ou "desculpa" para aumentar a probabilidade da vítima divulgar informações confidenciais, sendo parte importante dos ataques de *vishing*.

Por exemplo, a vítima recebe um telefonema de alguém que diz ser um gestor ou alguma autoridade (*impersonation*), e sob a desculpa de que está a prepar uma surpresa especial para um colaborador, pede acesso a algum sistema ou informações que as quais supostamente teriam o direito de saber.

Para evitar este tipo de ataque, o primeiro passo é assumir que ele sempre é uma possibilidade e além disso é sempre importante confirmar a identidade de quem lhe contacta, antes de passar a informação solicitada.

Não morda o isco!

A técnica conhecida como *baiting* consiste em explorar a curiosidade humana, a partir de dispositivos físicos como pen-drives, CDs e DVDs, para infectar o sistema do colaborador.



Imagine que um colaborador encontrou um *pen-drive* na sua caixa de correio ou no chão do parque perto do seu carro. Com a curiosidade de saber do que se tratava, acabou por conectá-lo ao PC da sua empresa e abre algum ficheiro desconhecido, que parecia uma música, que estava nele.

Neste caso, o colaborador foi vítima num esquema de *baiting*, e comprometeu a segurança da sua organização, que poderia ser afetada por exemplo com um ataque de *ransomware*.

Sendo assim, é necessário estar atento para não se deixar levar pela curiosidade. Caso note algum evento estranho, não deixe de informar odepartamento responsável da sua organização.

Métodos de prevenção

Como dito anteriormente, é necessário cultivar a cultura de segurança da informação dentro das organizações, para que os colaboradores tenham a noção de que podem participar ativamente no processo.

As medidas de prevenção como por exemplo software de segurança não são suficientes se os colaboradores não forem sensibilizados para as preocupações com *social engineering*. Isto porque muitas vezes a vulnerabilidade está no mundo físico e os ataques são iniciados das mais variadas formas, como um simples telefonema.

Portanto, as formas mais eficazes de combate ao *social engineering* são simulações, educação (formações) e criação de protocolos de segurança para informações sensíveis, pois assim os colaboradores estarão atentos e informados, mais preparados para agir caso notem algo suspeito.

5. Conecte-se sempre à rede privada da sua organização

Virtual Private Networks (VPNs) são redes privadas que permitem que o colaborador aceda à rede da sua organização a partir de casa, ou qualquer lugar fora do escritório, de forma segura.

5 razões para a utilizar sempre a VPN:

1. Permite o acesso remoto à infraestrutura da empresa a qualquer hora e lugar;
2. Está no "Manual do Colaborador" de muitas empresas, como boa prática;
3. Impede a intercetação de dados do tráfego com encriptação;
4. Protege a sua conexão enquanto utiliza uma rede doméstica ou pública;
5. Permite a autenticação segura via fator de localização (como visto anteriormente), para aceder sites e ferramentas.

Mais razões para utilizar a VPN

Geralmente as organizações são responsáveis por disponibilizar este tipo de ferramenta aos seus colaboradores e inclusive muitas das ferramentas e aplicações internas só podem ser acedidas através da VPN, entretanto, cabe ao colaborador utilizá-la.

A Eurotux sugere que a VPN da sua empresa seja utilizada sempre que possível, mesmo que não vá necessariamente aceder aos sistemas internos. Uma vez que as VPNs também ocultam o tráfego do utilizador do seu provedor de serviço de intenet (ISP), esta é uma boa ferramenta para manter a confidencialidade da informação.

Agora que já vimos a importância da rede privada da sua organização, o próximo tema será a segurança do ambiente de comunicação.

6. Tenha um ambiente de comunicação seguro

Durante o mês de Março de 2020, período de quarentena do coronavírus, uma plataforma emergiu como primeira opção entre aqueles que tiveram que recorrer à videoconferência.

Junto com o aumento do número de inscritos no Zoom, cresceu também a quantidade de incidentes de segurança e privacidade.

Vulnerabilidades do Zoom

A simplicidade do *setup*, uma das suas características principais, faz com que seja fácil ter a sua sala invadida por pessoas indesejadas. Estes episódios ficaram conhecidos como "*zoom-bombings*", onde os invasores atrapalham as reuniões, sobretudo as públicas.

Algumas vulnerabilidades, como a falha que permitia o *hacker* controlar remotamente qualquer PC com Windows 7 ou anteriores instalado, e as falhas que permitiam a infecção por *malware* a partir de .gifs e .zips enviados por *chat*, foram resolvidos.

Entretanto especialistas alertam para outras vulnerabilidades como a facilidade de se encontrar gravações das reuniões na *cloud* a partir da url, e a possibilidade de serem legítimas as vulnerabilidades críticas à venda na internet. Além disso foi constatado em Abril que utilizavam uma qualidade de encriptação inferior à declarada.

Estas vulnerabilidades podem comprometer a segurança da informação sensível da sua organização, então é importante conhecer outras soluções de vídeoconferências. No próximo tópico vamos abordar as ferramentas de escolha da Eurotux.

Escolha uma opção open-source de videoconferência segura

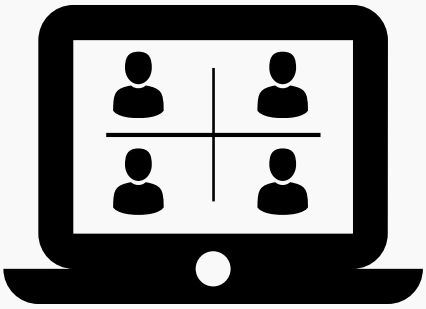
No contexto do teletrabalho é fundamental manter a segurança das comunicações e armazenar dados e informações críticos dentro do servidor da própria organização. As ferramentas organizacionais estão mais seguras quando é necessário utilizar a VPN para acedê-las.

O Jitsi Meet é uma opção *open-source* totalmente encriptada, utilizada pela Eurotux, que dispensa *download* de aplicações na versão para computador pois funciona diretamente nos *browsers*, seja no Linux, Windows ou macOS.

Uma sugestão é organizar vários ambientes, para cada departamento ou finalidade, para que as equipas sob regime de teletrabalho possam reunir-se sempre no mesmo url.

Sendo ***open-source***, como já sabemos, é possível personalizar o Jitsi de acordo com as necessidades organizacionais. Além disso esta característica garante a fiabilidade, baixos custos e escalabilidade.

Além do Jitsi, há muitas outras opções de software de videoconferênciacomo o Microsoft Teams e o Cisco Webex, que podem ser utilizadas. No entanto, várias destas têm como principal desvantagem o seu custo, dado que são software proprietário.



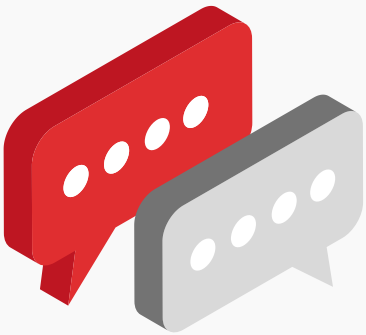
Escolha uma opção open-source de chat segura

A Eurotux utiliza e recomenda a plataforma de chat open-source Rocket.Chat. Como o Jitsi, o Rocket pode ser instalado na *cloud* ou alojado no servidor da sua organização, acessível por VPN, mantendo as comunicações seguras.

Além disso o código do Rocket.Chat está no GitHub, sendo possível personalizá-lo de acordo com as necessidades da sua organização. Está disponível para macOS, Windows e Linux.

Os recursos ilimitados são muitos, como 2FA, criptografia *end-to-end* (E2E), conferência de áudio e vídeo, compartilhamento de tela e ficheiros, possibilidade de organizar diversos canais e outras funcionalidades.

Outra vantagem de utilizar o Rocket e o Jitsi, é a integração que permite fazer uma video chamada *peer-to-peer* diretamente no Rocket.



Conclusão

Depois de conhecer os tipos de ameaças à segurança da informação, as táticas usadas por criminosos, além de boas práticas para as identificá e evitar, está sem dúvida mais preparado(a) para garantir uma maior segurança da informação da sua empresa, enquanto trabalha a partir de casa.

Outro fator importante do home office consiste em saber separar bem as atividades que serão desempenhadas nos equipamentos da organização, e as atividades que serão realizadas nos equipamentos pessoais. Isto significa não utilizar o equipamento destinado a trabalho para aceder redes sociais ou fazer compras online, por exemplo.

A VPN também deverá ser de utilização exclusiva no equipamento da sua organização, e não deverá ser configurada no seu equipamento pessoal. Caso necessite de apoio e orientação adicional para implementar medidas de segurança, recorra ao departamento de informática da sua empresa. Adotar uma cultura de segurança da informação é um processo que requer colaboração de todos. Se chegou até aqui, a Eurotux agradece e espera que este guia tenha ajudado a orientá-lo para esta cultura.

Conheça os Serviços da Eurotux para empresas: apoio na conceção, implementação e manutenção das suas infraestruturas informáticas.