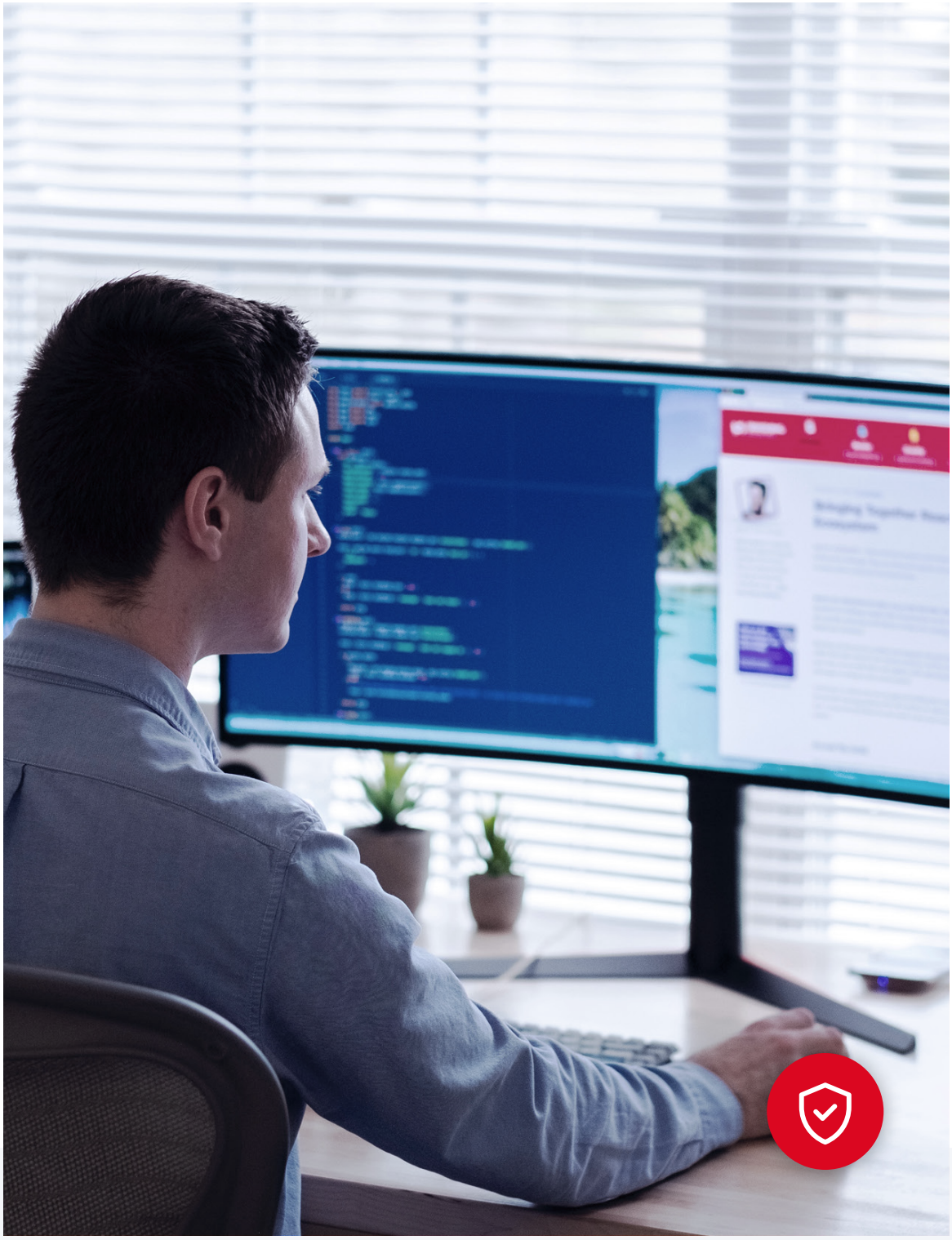
eurotux

MOVING BUSINESS FORWARD



Eurotux

GUIA DE SEGURANÇA NO TELETRABALHO

SAIBA COMO PROTEGER A SUA EMPRESA REMOTAMENTE EM 6 PASSOS.

ÍNDICE

MOVING BUSINESS FORWARD

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 está ligada à 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, circula 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.

De uma forma didática, este guia pretende ajudar as empresas ou instituições a transmitirem aos seus colaboradores boas práticas de segurança a adotar, para, em conjunto, se protegerem contra ataques informáticos e roubos de informação. São 6 passos simples e algumas ferramentas de trabalho remoto que a Eurotux recomenda como forma de aumentar a segurança da informação.

IMPORTÂNCIA DE PROTEGER A INFORMAÇÃO

A segurança de toda a informação de uma empresa é algo impossível de sobrevalorizar. Ela inclui dados pessoais, dados financeiros, estratégias de negócio, comunicações e todos os demais documentos que fazem parte da vida quotidiana de uma empresa. Quando estes dados são roubados, pode ser necessário pagar valores muito elevados para os recuperar, ou, se calhar, mais grave, podem cair diretamente nas mãos de concorrentes, ou serem 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;
- Cifra os dados, tornando-os ilegíveis, 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, eles devem ser muito bem protegidos.

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

TIPOS DE AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

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

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

As ameaças podem partir de agentes maliciosos externos, tais como *malware* ("vírus"), presentes em ficheiros corrompidos e recebidos por algum canal de comunicação (email, SMS, WhatsApp e *downloads*).

A ameaça pode também ter origem em métodos de social *engineering* (tema do Passo 4), muitas vezes utilizados como partes dum plano maior para roubar informações ou aceder a sistemas críticos.

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

EXEMPLO: A BITCOIN

Em casos de *ramsonware*, as organizações que tenham um bom sistema de *Backup* (cópias de segurança dos dados) estão salvaguardadas relativamente à perda de dados, embora enfrentem o risco de verem os seus dados expostos na Internet.

BOAS-PRÁTICAS DE CIBERSEGURANÇA EM 6 PASSOS

Este guia alerta para vulnerabilidades habitualmente exploradas pelos cibercriminosos (*hackers*) e sugere algumas das melhores práticas para reduzir a probabilidade de se ser vítima de um ataque informático. Segue uma lista de 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. Atenção aos sinais de burla
5. Conecte-se sempre à rede privada da sua organização
6. Tenha um ambiente de comunicação seguro

1 - UTILIZE *SOFTWARE* ATUALIZADO E DE CONFIANÇA

PARA AS EMPRESAS

O primeiro passo para uma empresa proteger a sua informação é assegurar que os sistemas operativos e o *software* utilizado são adequados e necessários às funções dos colaboradores. Além disso, uns e outros devem estar devidamente atualizados e com os *patches* de segurança em dia.

As soluções de segurança existentes atuam a vários níveis: na deteção de vulnerabilidades, no bloqueio de mensagens, emails ou ficheiros maliciosos (*malware*), na reparação dos seus danos, e ainda na identificação de possíveis eventos futuros.

PARA OS COLABORADORES EM TELETRABALHO

Além de os colaboradores em teletrabalho deverem ter o *software* adequado instalado no seu computador, é necessário que o mesmo esteja atualizado. Desta forma, eventuais problemas de segurança que poderiam ser explorados por hackers estarão mais salvaguardados.

Sempre que o colaborador em teletrabalho receba alguma mensagem a indicar que o *software* deve ser atualizado, a empresa deverá ser informada e deverão ambos, empresa e colaborador, agir no sentido de procederem à respetiva atualização.

5 ALIADOS DA EUROTUX PARA A CIBERSEGURANÇA

- **Proteção de *Endpoint***: Intercept X Endpoint - Um poderoso aliado contra *Malware, Ransomware, Exploits* e Vírus.
- ***Anti-Phishing***: Sophos Phish Threat - Simulações de ataque de *Phishing* e formação para os colaboradores.
- **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.
- **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.
- ***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 do teclado	123456789 112 123123
Utilizar as *passwords* que os sites sugerem (*default passwords*) - 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

MOVING BUSINESS FORWARD

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 aconselham o uso de *passwords* com 12 caracteres, e de preferência conter pelo menos:

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

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

FRASE	*PASSWORD*	INSPIRAÇÃO
"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

PROTEGER-SE DO MÉTODO *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. O método consiste no uso de um *software* que funciona por tentativa e erro de inúmeras combinações e *passwords* conhecidas diferentes, sucessivamente até encontrar a correta.

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.

A utilização destas **dicas para definir uma boa *password*** 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, tal como um dicionário, até encontrar a *password* em questão.

Para diminuir a probabilidade de uma *password* ser descoberta num *dictionary attack*, deve optar-se 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. Para colmatar esta limitação têm surgido ao longo dos anos vários métodos como o que se descreve a seguir.

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;

Encontre a palavra correspondente na lista de palavras;

```
Diceware index

41253   lockout
41254   locucao
41255   logica
41256   lodo
41257   local
```

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

Ex.: lodo carro baleia memória vampiro

Pronto! Por esta via, obtem-se uma *passphrase* com muitos *bits* de entropia, difícil de ser quebrada pelos métodos tradicionais. Logo que ela faça sentido para o utilizador, ela será facilmente memorizada.

GUARDAR AS *PASSWORDS*

Anotar em papel cada *password* de cada um dos 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. 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 tem limite de dispositivos ou de *passwords*. Além disso, aceita a 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 gestor de *passwords open-source* e colaborativo, que permite a partilha de credenciais. Utiliza diversos níveis de cifragem. Além disso, os dados ficam armazenados no servidor *web* da própria organização.

3 - ATIVE A AUTENTICAÇÃO EM DUAS ETAPAS

Como se viu no tópico anterior, as *passwords* podem ser facilmente comprometidas, recorrendo a métodos como o *Brute Force* e o *Dictionary Attacks*. Por conseguinte, é recomendável, senão imprescindível, 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 pelo qual o acesso só é fornecido mediante 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.
- **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. Fatores de conhecimento, como respostas a perguntas de segurança por exemplo, podem ser conhecidos por determinadas pessoas ou podem ser investigados nas 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 ALGO 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, das quais são exemplos Free OTP, Microsoft Authenticator e Google Authenticator.

Os telemóveis também são amplamente utilizados como fator de posse, através de autenticação *push* ou via SMS. Os telemóveis estão, porém, sujeitos a serem clonados e usados indevidamente. Para colmatar essa vulnerabilidade, cresce a 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 O TIPO DE MFA QUE É ACONSELHÁVEL PARA CADA ORGANIZAÇÃO?

Para obter um maior grau de segurança, a Eurotux aconselha que, sempre que possível, se utilize no mínimo a 2FA para permitir o acesso remoto à informação crítica para a empresa. Uma implementação tipo deste nível de proteção implicaria, por exemplo, a introdução de uma *password* e o fornecimento de outro fator de autenticação, eventualmente um *token*, via SMS, OTP ou localização.

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

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

Estas barreiras ao acesso indevido à informação e às 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*.

4 - ATENÇÃO AOS SINAIS DE BURLA

As ações e o 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 que comprometeu as ferramentas administrativas do Twitter de Julho de 2020, tiveram origem em práticas de *social engineering*, e poderiam ter sido evitados com uma maior educação dos colaboradores, ou com a implementação de uma 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 de levar a vítima a realizar determinadas ações, depois utilizadas por cibercriminosos para obter acessos privilegiados ou iniciar ataques subsequentes. 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-se como algum colaborador do suporte técnico e pedir, com senso de urgência, que se insira algum comando no seu PC. Neste caso, a pressão faz com que a vítima tome uma ação precipitada, sem verificar as credenciais do suposto colaborador, ficando vulnerável ao roubo de dados ou à invasão do seu 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 credenciais ou de dados de cartões de crédito, geralmente via email (em nome de um banco ou outro serviço). É solicitado que seja feito o *login* numa página réplica falsa de uma instituição e que regista (contra a vontade do utilizador) os dados inseridos. Podemos ainda distinguir *spear phishing*, quando os emails são cuidadosamente personalizados e enviados para poucas pessoas selecionadas, enquanto no *phishing* em massa, são enviados sem personalização para o maior número de pessoas possível.

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

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

COMO DETETAR ATAQUES DE *PHISHING*?

De acordo com a Sophos, 41% das organizações sofrem tentativas de *phishing* diariamente, e mais de três quartos (77%) pelo menos uma vez por mês. É, pois, 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;
- Consequências graves, caso não faça o que pedem;
- Palavras fortes e enervantes (como "A sua conta foi violada!");
- Saudações genéricas (Ex.: "Caro cliente");
- Solicitação de dados e informações pessoais e organizacionais sensíveis.

É ainda possível que os criminosos utilizem alguma informação pessoal obtida através das redes sociais para personalizar o email e torná-lo convincente.

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

A melhor forma de prevenção que os administradores têm contra o *phishing* é fazendo simulações e dando formação, de forma a que os colaboradores aprendam a identificar possíveis ataques. Além dessas ações, também se recomenda que haja proteção dentro das plataformas de email.

ATENÇÃO A POSSÍVEIS ATAQUES DE *PRETEXTING*

Os ataques de *pretexting* (pretexto) ocorrem quando os criminosos criam algum cenário fictício ou "desculpa" para aumentar a probabilidade de a 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*). Sob a desculpa de que está a preparar uma surpresa especial para um colaborador, é pedido acesso a algum sistema ou informações, supostamente do conhecimento da vítima.

Para evitar este tipo de ataque, o primeiro passo é assumir que ele sempre é uma possibilidade, e, com isso em mente, confirmar a identidade do nosso interlocutor antes de passar a informação solicitada.

NÃO MORDER 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 infetar o sistema do colaborador.

Imagine-se a seguinte situação. Um colaborador encontrou uma *pen-drive* na sua caixa de correio ou no chão perto do seu carro. Com a curiosidade de saber do que se tratava, esse colaborador conectou o dispositivo ao PC da sua empresa e abriu um ficheiro desconhecido, que parecia uma música, que estava nele. Neste caso, o colaborador tinha sido vítima num esquema de *baiting* e tinha comprometido a segurança da sua organização, por exemplo com um ataque de *ransomware* oculto nesse ficheiro.

É, pois, manifesta a necessidade de estar atento para não se deixar levar pela curiosidade. Na ocorrência de algum evento estranho, a primeira atitude a ter é informar o departamento responsável.

MÉTODOS DE PREVENÇÃO

Como já se disse, é necessário cultivar uma cultura de segurança da informação dentro das organizações, para sensibilizar os colaboradores de que eles podem e devem participar ativamente no processo.

As medidas de prevenção, como por exemplo a utilização de *software* de segurança, não são suficientes, se os colaboradores não forem sensibilizados para as preocupações com *social engineering*. Muitas vezes a vulnerabilidade está no mundo físico, e os ataques são iniciados das mais variadas formas, como um simples telefonema, cujas consequências o mais evoluído *software* pode não impedir.

Portanto, as formas mais eficazes de combate ao *social engineering* são simulações, educação (formações) e criação de protocolos de segurança para informações sensíveis. Colaboradores atentos e informados estão 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 de qualquer lugar;
2. Está no "Manual do Colaborador" de muitas empresas, como boa prática;
3. Impede a interseção de dados do tráfego com encriptação;
4. Protege a conexão enquanto se utiliza uma rede doméstica ou pública;
5. Permite uma autenticação segura via fator de localização, para aceder a sítios da internet e a ferramentas online.

MAIS RAZÕES PARA UTILIZAR A VPN

Geralmente as organizações são responsáveis por disponibilizar este tipo de ferramenta aos seus colaboradores, e, inclusivamente, muitas das ferramentas e aplicações internas só podem ser acedidas através da VPN. No entanto, é da responsabilidade do colaborador utilizá-la.

A Eurotux sugere que se utilize uma VPN 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 internet (ISP), esta é uma boa ferramenta para manter a confidencialidade da informação.

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 às videoconferências, a Zoom.

Junto com o aumento do número de inscritos na plataforma, 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 ao *hacker* controlar remotamente qualquer PC com Windows 7 instalado (ou versões anteriores), e as falhas que permitiam a infeção por *malware* a partir de .gifs e .zips enviados por chat, foram resolvidos.

Entretanto, alguns especialistas alertam para outras vulnerabilidades como a facilidade de se encontrar gravações das reuniões na *cloud* a partir do endereço web. Além disso, em abril de 2020 verificou-se que a plataforma utilizava uma qualidade de encriptação inferior à declarada.

Estas vulnerabilidades podem comprometer a segurança da informação sensível das organizações. Com esta questão em mente, a Eurotux sugere outras soluções de videoconferências.

UMA OPÇÃO *OPEN-SOURCE* DE VIDEOCONFERÊNCIA SEGURA

Em 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 para o conseguir ficam 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. Ela funciona diretamente nos *browsers*, seja em ambientes Linux, Windows ou macOS.

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

Sendo uma plataforma ***open-source***, como é sabido, é possível personalizar o Jitsi de acordo com as necessidades organizacionais. Por outro lado, fiabilidade, baixos custos e escalabilidade estão garantidos desde logo.

Além do Jitsi, há muitas outras opções de *software* de videoconferência, como o Microsoft Teams e o Cisco Webex. No entanto, algumas destas opções têm como principal desvantagem o seu custo, dado que são *software* proprietário.

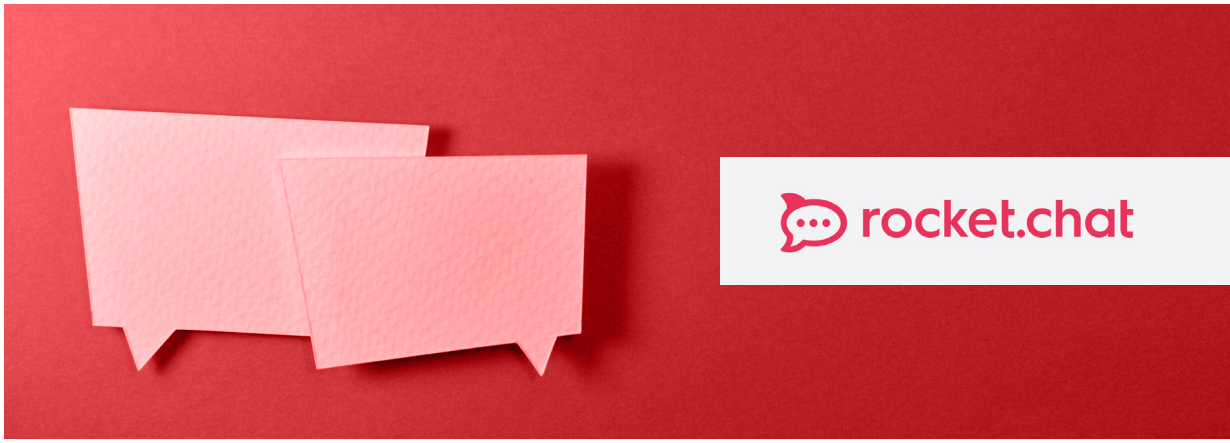
UMA OPÇÃO *OPEN-SOURCE* DE *CHAT* SEGURA

A Eurotux utiliza e recomenda a plataforma de chat open-source Rocket.Chat. Tal como o Jitsi, o Rocket pode ser instalado na *cloud* ou alojado no servidor da 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 de cada organização. Está disponível para macOS, Windows e Linux.

Os recursos disponíveis no Rocket.Chat são muitos: 2FA, criptografia *end-to-end* (E2E), conferência de áudio e vídeo, partilha do ecrã e ficheiros, possibilidade de organizar diversos canais, entre outras funcionalidades.

Uma última vantagem que vale a pena referir na utilização do Rocket.Chat e do Jitsi, é a integração que permite fazer uma videochamada *peer-to-peer* diretamente no Rocket.Chat.



CONCLUSÃO

Conhecer os vários tipos de ameaças à segurança da informação, as táticas usadas por criminosos, as boas práticas para identificar e evitar umas e outras, é fundamental para criar ambientes com maior segurança da informação das empresas, enquanto se trabalha remotamente.

Uma avaliação importante a realizar na configuração do *home office* é a separação das atividades que serão desempenhadas nos equipamentos da organização das atividades que serão realizadas nos equipamentos pessoais. Isto significa que não se pode utilizar o equipamento destinado a trabalho para aceder a redes sociais ou fazer compras *online*, por exemplo.

A VPN também deverá ser de utilização exclusiva no equipamento da organização, e não deverá ser configurada nos equipamentos pessoais.

Caso seja necessário apoio e orientação adicional para implementar medidas de segurança, deve sempre recorrer-se ao departamento de informática da empresa. Adotar uma cultura de segurança da informação é um processo que requer a colaboração de todos.

A Eurotux agradece e espera que este guia tenha ajudado a divulgar esta cultura.

CONHEÇA OS SERVIÇOS DA EUROTUX PARA EMPRESAS: APOIO NA CONCEÇÃO, IMPLEMENTAÇÃO E MANUTENÇÃO DAS SUAS INFRAESTRUTURAS INFORMÁTICAS.