.dream
DIGITAL MANAGEMENT

Manual de boas práticas na utilização de recursos tecnológicos

AGOSTO 2019 V1.0

A utilização de tecnologia na empresa

No nosso dia a dia somos confrontados com a necessidade de utilizar tecnologia nas mais variadas situações. Usamo-la de forma completamente natural, muitas vezes sem nos apercebermos, ficando frequentemente expostos a ameaças inerentes ao seu uso.

No mundo empresarial, esta realidade não é diferente. Acresce aqui o facto de haver uma interação frequente entre membros da mesma empresa e entre membros de empresas diferentes, aumentando assim a exposição às ameaças resultantes da utilização das tecnologias.

Embora o modo de utilização tenha uma correspondência direta com parte significativa dos problemas e ameaças com que somos confrontados, **o desconhecimento sobre procedimentos e mecanismos simples de prevenção assume também uma dimensão significativa** nesta problemática.

É neste contexto que no âmbito do projeto DreAM abordamos, sem ordem particular, um conjunto de aspetos e soluções que acreditamos poderem ajudar a mitigar muitos destes problemas.

As ferramentas e os sistemas de informação

Na era da informação, em que vivemos, torna-se indispensável a utilização de dispositivos computadorizados. Desde o telefone móvel até ao computador de mesa, passando pelo sistema de assiduidade ou pelo sistema de video-vigilância, todos assentam o seu funcionamento em sistemas operativos e aplicações.

Tratando-se de ***software* que foram pensados e implementados por seres humanos, os mesmos contêm frequentemente *"bugs"*, que são mais tarde detetadas e corrigidas.**

Enquanto não são corrigidos, estes *bugs* podem conduzir a dois tipos de situações distintas:

— Mau funcionamento do sistema ou da aplicação, podendo no limite colocar em risco ou introduzir resultados inesperados na operação em que está envolvido. Pensemos, por exemplo, nas implicações geradas por um sistema de controlo de elevadores que, em determinadas condições, apresente um funcionamento errático, ou no sistema de gestão das contas de um banco que, em condições específicas, manifeste um qualquer erro no cálculo de uma operação bancária.

— Estando aparentemente a funcionar bem, o *bug* pode ser explorado por alguém que previamente o tenha identificado. Aqui a falha pode ser utilizada para, de forma camuflada, controlar ou executar ações que comprometam as suas credenciais ou a informação armazenada no sistema em causa. Este tipo de uso indevido pode, muitas vezes, chegar ao ponto de **o sistema da vítima ser utilizado para escutar ou roubar credenciais de outros intervenientes que se liguem na mesma rede de dispositivos**. É fácil, neste caso, imaginar o interesse em ter controlo, por exemplo, de um sistema de gestão de acessos físicos ou do sistema de video-vigilância de um edifício.

No contexto do roubo de credenciais ou de informação sensível, podemos imaginar o interesse em conseguir aceder ao sistema de *homebanking* de uma pessoa ou de uma empresa, em roubar os planos de desenvolvimento de um produto inovador que poderá vir a ser líder de mercado, ou em escutar

as comunicações entre determinada empresa e os seus parceiros e fornecedores, por forma a antecipar medidas concorrenciais que combatam essa novidade.

Tendo como fundamento o até agora exposto, **devemos a todo o custo garantir que os nossos sistemas estão atualizados e têm aplicadas todas as correções disponíveis para cada um deles**.

Nem sempre a aplicação destas atualizações é inócua e, sob a pressão de ter que ter os sistemas em funcionamento, somos levados a equacionar remeter para segundo plano a necessidade de aplicação dessas atualizações. Este é um erro comum que deve ser evitado, questionando e pressionando os fornecedores dos sistemas afetados a desenvolverem também, eles próprios, esforços no sentido de compatibilizar os sistemas que fornecem com as versões novas dos sistemas com que interoperam.

Potenciada pelo facto de estarem acessíveis sem qualquer custo, há uma tendência para a utilização de versões de certos *software*, e até mesmo de sistemas operativos, descarregados da internet a partir de localizações sem qualquer controlo. Esta é uma prática a evitar, por duas razões distintas: por um lado, tanto quem distribui como quem descarrega, incorre no crime de pirataria informática, por outro lado, fica à mercê de "funcionalidades extra", que poderão ser introduzidas intencionalmente para posteriormente serem utilizadas com o objetivo de controlar ou roubar informação dos sistemas onde estes *software* são instalados.

Outros aspetos importantes na gestão dos sistemas que usamos, prendem-se com a forma como lidamos com a informação e credenciais dos acessos que nos são facultados, com a forma como usamos os recursos de internet, como usamos ferramentas de comunicação como o e-mail ou como lidamos com a informação que vamos produzindo.

Estes e outros assuntos são alvo de uma análise mais detalhada nas próximas secções.

A gestão de acessos e credenciais

Com o crescente número de sistemas e aplicações que usamos diariamente, torna-se praticamente impossível memorizar todos os detalhes necessários para efetuar os vários acessos. Há alguma tendência, por isso, para utilizar os mesmos códigos em múltiplos acessos por forma a facilitar a gestão de credenciais. Esta é uma prática a evitar, pois **uma vez descoberto um destes códigos, múltiplas plataformas ou recursos ficarão imediatamente comprometidos**.

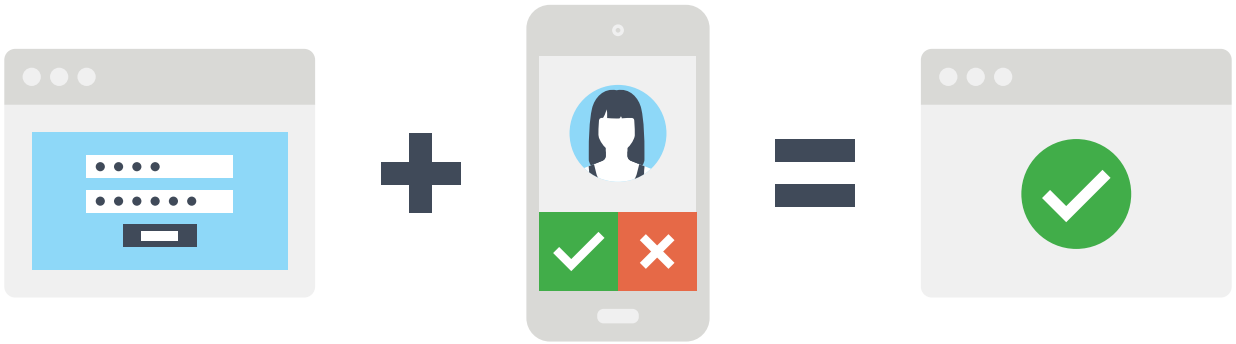
Outra medida comum, é a anotação destes códigos, mas também aqui temos que ter em atenção as questões que se prendem com a exposição do meio em que fazemos essas anotações.

Embora tenhamos a noção de que as notas em papel sejam convidativas pela aparente grande facilidade de as utilizar, esta é uma muito má prática e, por isso, a evitar. Mesmo recorrendo a mecanismos de "disfarce", para um interessado motivado e com alguma prática, esses mecanismos são facilmente ultrapassáveis e decifráveis.

Outra abordagem que encontramos, frequentemente, é a de registar este tipo de informação em ficheiros de texto ou folhas de cálculo. Consideravelmente mais segura, esta metodologia também deve ser evitada pois não nos protege dos olhares mais indiscretos quando nos ausentamos dos nossos postos de trabalho sem proteger o acesso ao computador.

Ainda que possamos tentar esconder esta informação numa área menos óbvia, estes dados ficam completamente expostos em caso de furto ou de necessidade de reparação do equipamento em que a guardamos.

Por forma a resolver este problema, estão disponíveis múltiplas opções dos denominados gestores de senhas. Existem soluções comerciais e soluções gratuitas, estando as principais diferenças associadas a funcionalidades, a uma maior ou menor facilidade de utilização ou à sua disponibilidade num maior ou menor número de plataformas tecnológicas.



Privilegiando as soluções baseadas em código aberto, em que o escrutínio da qualidade do programa é bastante mais abrangente que nas soluções fechadas ou proprietárias, sugere-se a utilização do *KeepassC*.

Ainda com o propósito da boa gestão de credenciais e acessos, deve ser sempre posta em causa toda e qualquer solicitação de fornecimento de dados de acesso, fora do contexto de uso das aplicações. Mesmo que o pedido aparente ser fidedigno, por e-mail ou outra via, os responsáveis pela gestão dos recursos ou aplicações nunca têm necessidade de saber as credenciais dos utilizadores e, neste contexto, **tais acessos nunca devem ser fornecidos a terceiros**.

Uma nota adicional para chamar a atenção de que, cada vez mais, as aplicações que usamos no dia a dia apresentam a possibilidade de ativação de múltiplos fatores de autenticação. Estes, embora numa primeira fase possam parecer um entrave ou complicação na utilização do recurso que se pretende, são na realidade um grande incremento na proteção do acesso indevido a informação ou recursos, por parte de terceiros, não autorizados.

Além destas medidas de boa gestão dos acessos e códigos, há também aspetos a ter em conta, relacionados com a forma como acedemos e usamos as redes de dados.

A utilização das redes de dados

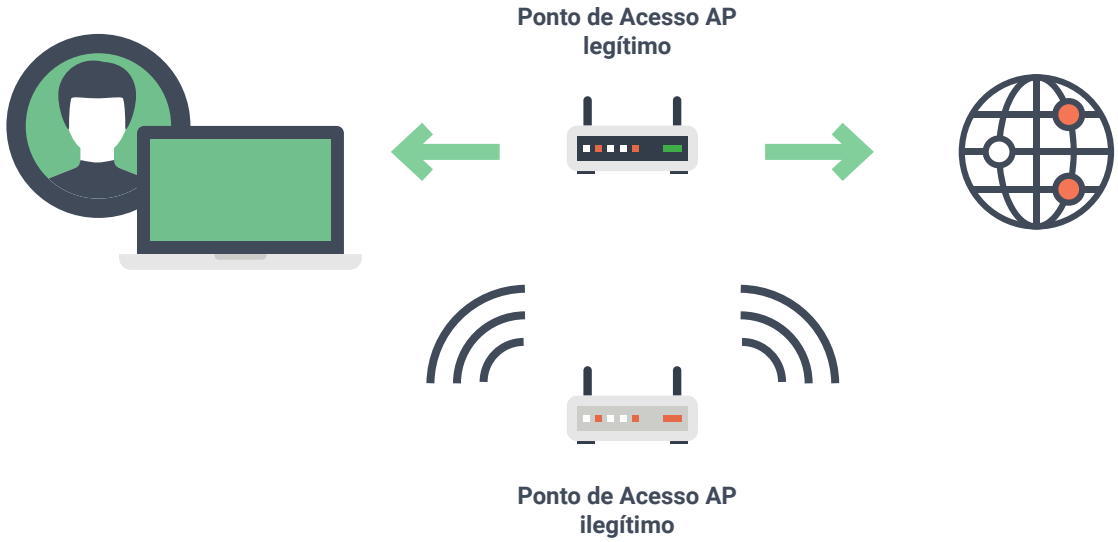
Desde há já alguns anos que o contexto tecnológico em que vivemos se centra na denominada internet, um recurso quase infinito, que se tornou a principal e preferencial via de comunicação. Através dela são feitas todo o tipo de comunicações e transações, tendo-se inclusivamente tornado no principal meio de divulgação de notícias e informações urgentes.

Quer num contexto mais pessoal, quer num contexto profissional, ao "navegar" na internet, somos a toda a hora assediados com todo o tipo de ofertas. Mas, também aqui, umas são mais bem-intencionadas que outras e, por isso, devemos estar atentos a um conjunto de ameaças.

Assim, elencamos um conjunto de medidas genéricas que permitem uma maior e melhor proteção durante a utilização de redes locais ou da própria internet:

— **É de extrema importância a utilização de mecanismos de proteção nas comunicações. O uso de SSL ou TLS**, nomeadamente na transferência de dados sensíveis (momento da autenticação e no envio ou recebimento de informação, de modo generalizado) é fundamental. No caso da utilização de um "navegador" (MS Edge, Chrome, Firefox, Safari ou outro) o acesso seguro é demonstrado pela figura ativa de um cadeado. Embora não seja tão simples de verificar a sua utilização neste caso, o uso de SSL ou TLS é também mandatório em clientes de e-mail.

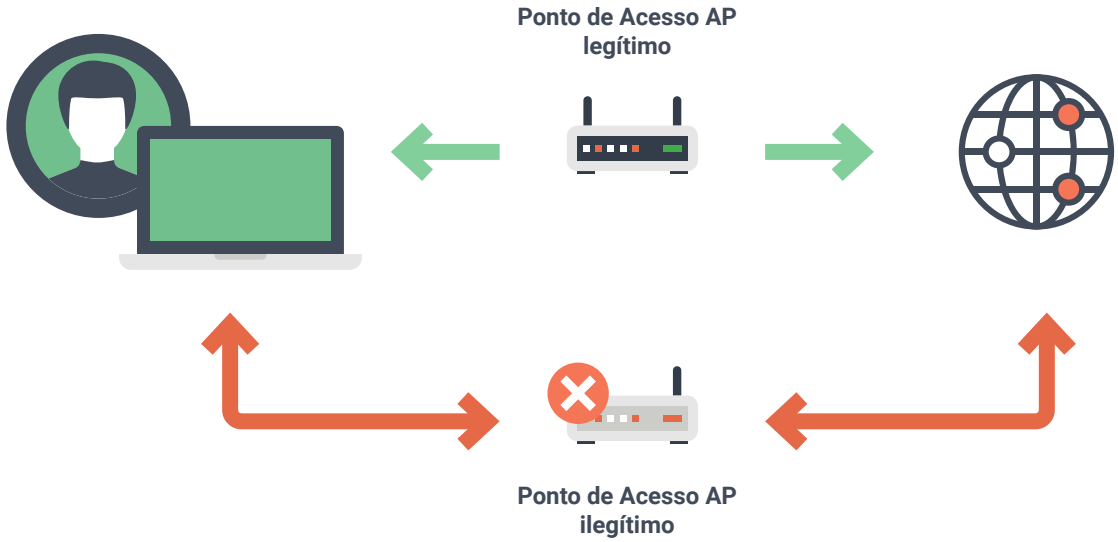
— **Todos os equipamentos devem ter a proteção de antivírus ativa.** Este é um recurso que pode travar ataques que muitas vezes ainda não tiveram divulgação pública.



— À semelhança do que já foi referido, com maior enfase para o sistema operativo, é de extrema importância usar navegadores atualizados. Há inúmeros vetores de ataque que são evitáveis se usarmos as versões mais recentes destas ferramentas de pesquisa e consulta de informação.

— Por último, **é mandatório ativar a proteção da rede (*firewall*) nos dispositivos**. Mesmo que o antivírus em uso, por alguma razão não tenha essa funcionalidade disponível, todos os sistemas operativos disponibilizam um nível simples de proteção desta natureza.

Em muitos dos locais a que nos dirigimos ou em que ficamos alojados, são disponibilizados acessos a redes sem fios. Muitas vezes estes acessos são geridos de forma displicente ou não são de todo geridos, criando ameaças que poderão surgir tanto do interior como do exterior (a tecnologia baseada em radiofrequência não é passível de limitar ao interior de um espaço ou edifício).



Neste contexto, há cuidados básicos a ter, quer do ponto de vista de quem usa (que complementam aspetos já expostos), quer do ponto de vista de quem oferece o serviço.

QUEM USA O SERVIÇO:

— Sempre que possível, usar o "*hotspot*" pessoal.

— Evitar usar redes sem fios que não tenham encriptação, privilegiando as que, no mínimo, ofereçam WPA ou WPA2.

— Nunca ligar a redes sem fios que apareçam anunciadas, mas cuja origem possa não ser a instituição ou local onde nos encontramos.

QUEM OFERECE O SERVIÇO:

— Pelo facto de oferecer o serviço de acesso à internet a indivíduos estranhos à instituição, surge a necessidade de segmentação e segregação da rede, em pelo menos duas: a usada pela instituição, e a usada pelos visitantes. Sem esta segmentação, qualquer comprometimento ou vulnerabilidade de um visitante, coloca imediatamente em risco toda a rede com que este comunica.

— Na configuração do acesso que se oferece, há necessidade de escolha do protocolo mais seguro disponível. No caso de existir, deverá ser, pelo menos, WPA2.

A colocação de um código de acesso para uso dessa rede sem fios é também uma obrigatoriedade, não devendo este código ser óbvio e, na medida do possível, ser trocado com alguma frequência.

A utilização do e-mail

Sendo um *standard*, de entre os meios preferenciais de comunicação, pessoal ou empresarial, este recurso não poderia ser uma exceção, no que respeita a cuidados a ter durante a sua utilização.

À semelhança de outros acessos que envolvem transferência de informação, há necessidade que estas transferências ocorram de forma segura e através de canal seguro. **Assim, a configuração do recebimento e envio de mensagens, nos programas cliente de e-mail, deve obrigatoriamente usar SSL ou TLS**, mesmo que estes acessos sejam oferecidos pelo provedor de serviço, sem a obrigatoriedade do seu uso.

Em contexto empresarial, muitas das transações financeiras são antecedidas por comunicação, na maioria usando e-mail. Por essa razão, deve ser sempre feita uma verificação, usando uma segunda via ou canal, após um primeiro contacto ou quando há alteração de dados de contacto ou bancários.

Esta verificação reveste-se de particular importância quando as comunicações futuras implicam dados ou transações financeiras ou outra informação vital da empresa.

Sendo este canal usado globalmente, para todo o tipo de comunicação, é também o escolhido para uma variedade de ataques que têm como fim a obtenção de acessos ou dados.

Reitera-se a ideia de que é fundamental que todos **os utilizadores desta ferramenta dentro da empresa sejam instruídos no sentido de, em caso algum, fornecerem os seus acessos a terceiros.** Estes devem ter sempre muita atenção a **ligações presentes em e-mails que apontem para páginas de entrada de ferramentas que habitualmente usam. Este é um método bastante usado para a obtenção de credenciais de acesso**.

A gestão de recursos e dados na empresa

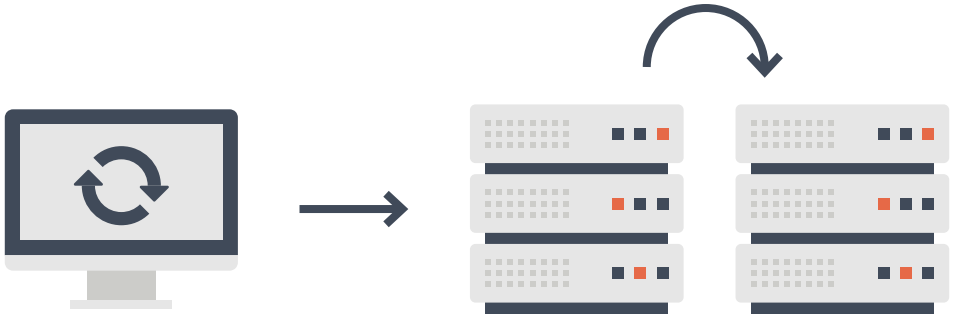
Começando por revisitar o e-mail, a utilização de endereços institucionais personalizados para a empresa, nas contas que gerem ou transacionam informação é uma prática a adotar. Além de uma maior credibilidade, ajuda os parceiros e os clientes a melhor identificarem qualquer tentativa de impersonificação em nome da empresa.

Uma medida adicional neste contexto, é aplicar nos e-mails assinaturas digitais qualificadas, como as que constam nos cartões de cidadão. Este tipo de assinatura permite validar, de forma inequívoca, o remetente.

À luz da legislação, em particular, no cumprimento de regras definidas pelo Regulamento Geral da Proteção de Dados, os colaboradores com endereço de e-mail "pessoal" no domínio da empresa, impede que este seja consultado por outra qualquer pessoa. Esta limitação impede que, por exemplo, durante as férias ou durante uma baixa, o endereço não possa ser consultado por algum membro da empresa.

Assim, é recomendável que os endereços relativos a áreas ou serviços da empresa devam ser criados de forma "despersonalizada", sem relação ao nome da pessoa que habitualmente gere esse endereço.

Embora o teletrabalho não seja muito comum em empresas fora da área tecnológica, este modelo passará progressivamente a ser aceite como uma forma natural de trabalho para algumas áreas da empresa. Uma abordagem que, com frequência, se encontra implementada é a de expor diretamente alguns serviços ou recursos, para que estes possam ser acedidos pelos colaboradores que trabalham fora da empresa. Esta é uma prática a evitar, pois expõe a empresa a riscos de ataque desnecessários. Em vez disso, deve ser criado um sistema de suporte a uma VPN, que permite que todos os utilizadores, com acesso, possam trabalhar com segurança a partir do exterior. Neste modelo, os seus utilizadores trabalham com se estivessem fisicamente na empresa.



Por fim, mas ainda assim de máxima importância, referimos a necessidade de implementar um sistema de salvaguardas, que garanta a reposição parcial ou integral de toda a informação da empresa, em caso de falhas simples ou mesmo de uma catástrofe.

Uma forma simples que é, frequentemente, apontada para garantir estas salvaguardas parece ser copiar os dados para discos ou partilhas na rede, em servidores distintos. **Infelizmente uma das ameaças que nos últimos anos se tem globalizado, o *ransonware*, veio mostrar uma grande fragilidade nesta abordagem, fazendo com que as próprias salvaguardas fiquem comprometidas**.

A solução é, por isso, garantir que o armazenamento das salvaguardas é feito numa camada ou numa rede diferente, à qual não há acesso de rede direto a partir dos servidores de produção. Por forma a garantir essa separação, existem múltiplos *software* disponíveis que fazem uso de um agente, e só esse agente comunica com o repositório, que não deve estar acessível diretamente a partir de qualquer parte o participante da rede.

Uma última nota para referir a importância de as salvaguardas estarem facilmente acessíveis em caso de necessidade e também da necessidade de testar estas salvaguardas com alguma frequência, por forma a garantir a sua integridade e utilidade.

Ligações úteis

CNCS — https://www.cncs.gov.pt/

RGPD — https://www.cnpd.pt/home/rgpd/rgpd.htm

Portal do Cidadão — https://www.autenticacao.gov.pt/

Glossário

BUG — Falha, defeito no programa, defeito no software.

SSL — Secure Sockets Laye — Protocolo de comunicação para implementação de camada de ligações seguras.

TLS — Transport Layer Security — Protocolo de comunicação, para implementação de uma camada de transporte de informação, de forma segura.

MS Edge — Navegador de internet da Microsoft.

Chrome — Navegador de internet da Google.

Firefox — Navegador de internet da fundação Mozilla.

Safari — Navegador de internet da Apple.

WPA — Wi-Fi Protected Access — Protocolo de acesso sem fios protegido.

WPA2 — Wi-Fi Protected Access v2 — Versão 2 do protocolo de acesso sem fios protegido.

VPN — Virtual Private Network — Rede privada que coloca, virtualmente, na rede da empresa, um computador em localização remota.

itecons

POCI-02-0853-FEDER-036380

dream.itecons.uc.pt

MORADA
Rua Pedro Hispano, s/n
3030-289 Coimbra

CONTACTOS
Tel: (+351) 239 79 89 49
E-mail: itecons@itecons.uc.pt

COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional