eBook

CIBERSEGURANÇA

SAIBA COMO PROTEGER A SUA EMPRESA

TELECOM

ÍNDICE

INTRODUÇÃO

O perigo espreita a cada nó da rede e os gestores já perceberam que é preciso estar permanentemente alerta. A exposição cibernética está a crescer à medida que as empresas se tornam mais dependentes da tecnologia e os ciberataques são realizados quando menos se espera. Apesar dos gestores estarem vigilantes e considerarem a cibersegurança uma prioridade de topo na gestão de riscos, hesitam na sua capacidade para gerir o risco de um ataque cibernético.

Um estudo mundial realizado recentemente pela consultora Marsh e pela Microsoft concluiu que a cibersegurança está entre as prioridades TOP5 de gestão de riscos. Dos 1300 inquiridos, uma grande maioria, mais precisamente 75%, identifica a interrupção do negócio como o cenário de perda cibernética com maior potencial para impactar a sua organização. Este valor pode comparar-se aos 55% que citaram a violação de informação de clientes, que historicamente tem sido o foco das organizações.

1. **65% DAS EMPRESAS PORTUGUESAS CONSIDERA QUE OS "ATAQUES CIBERNÉTICOS EM GRANDE ESCALA" SÃO O PRINCIPAL RISCO QUE O MUNDO PODERÁ VIR A ENFRENTAR EM 2018;**
2. **SEGUIDO DE "ATAQUES TERRORISTAS EM LARGA ESCALA", COM 42%;**
3. **OS "EVENTOS CLIMÁTICOS EXTREMOS" E "CRISES DE ÁGUA" SURGEM COM 39%;**
4. **COM 31%, AS "CRISES FISCAIS E FINANCEIRAS EM ECONOMIAS CHAVE";**
5. **AS "CATÁSTROFES NATURAIS", COM 24%.**

NO ESTUDO «A VISÃO DAS EMPRESAS PORTUGUESAS SOBRE OS RISCOS 2018», A MARSH DEMONSTRA QUE AS EMPRESAS PORTUGUESAS ESTÃO HOJE MAIS ALERTAS PARA O PAPEL QUE A GESTÃO DE RISCOS DEVE TER DENTRO DAS SUAS ORGANIZAÇÕES, SENDO QUE 40% (FACE A 35% EM 2017) AFIRMA DAR ELEVADA IMPORTÂNCIA A ESTA TEMÁTICA E 45% DAR SUFICIENTE IMPORTÂNCIA.

A Accenture confirma isso mesmo num estudo apresentado no primeiro trimestre deste ano. A consultora apurou que o número médio de ataques cibernéticos direcionados por organização mais do que duplicou este ano, em comparação com os 12 meses anteriores (232 até janeiro de 2018 versus 106 até janeiro de 2017). Tendo em conta este aumento de ameaças cibernéticas, as organizações estão a demonstrar um maior sucesso na deteção e bloqueio destas ameaças.

41%

DAS EMPRESAS AFIRMA TER AUMENTADO O VALOR ORÇAMENTADO PARA A GESTÃO DE RISCOS EM 2018, O QUE REPRESENTA UMA EVOLUÇÃO MUITO SIGNIFICATIVA QUANDO COMPARADA COM 2017 E COM 2016, 28% E 24% RESPETIVAMENTE.

Outra conclusão do estudo, é que as empresas demoram menos tempo a detetar uma quebra de segurança: passámos de meses e anos para dias e semanas. Em média, 89% dos inquiridos referiu que as suas equipas detetaram as infracões após um mês de terem ocorrido, enquanto que no ano passado apenas 32% das equipas conseguiram detetá-las nesse prazo. Este ano, 55% das organizações levaram uma semana ou menos a detetar uma infração, em comparação com 10% no ano passado.

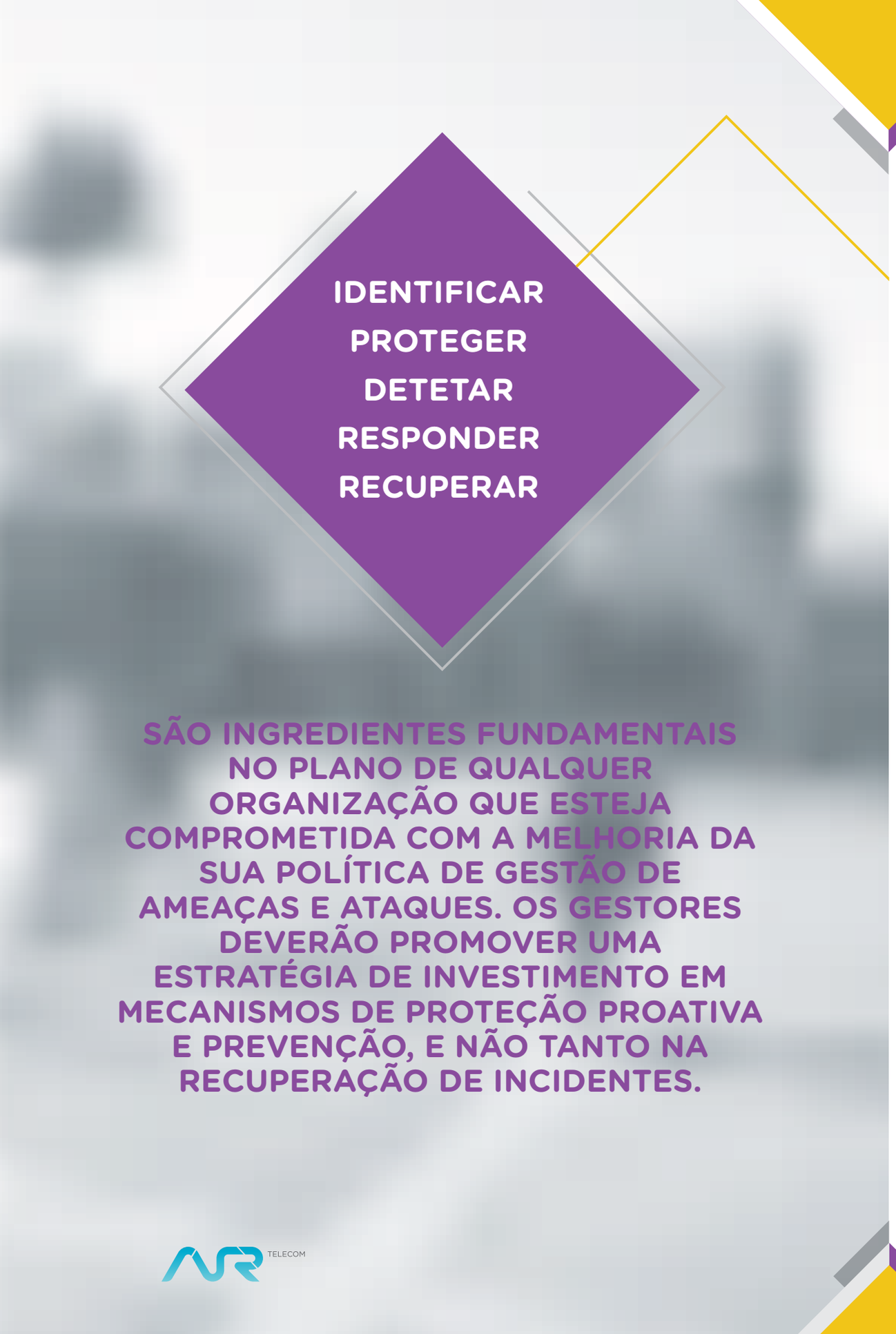
Este cenário traduz-se numa maior consciência dos gestores para estas temáticas e um abandono da postura de "deixar andar" que até aqui caracterizava a ação dos gestores.

O RGPD TAMBÉM CONTRIBUIU PARA ESTE DESPERTAR DE CONSCIÊNCIAS JÁ QUE COLOCOU NA RIBALTA A INFORMAÇÃO E OS DADOS COMO UM ATIVO VALIOSO QUE É PRECISO PROTEGER PARA BEM DO NEGÓCIO E DA CARTEIRA, JÁ QUE AS MULTAS POR NÃO CONFORMIDADE SÃO AVULTADAS.

Ainda assim, a Accenture explica que apenas duas em cada cinco empresas estão atualmente a investir em tecnologias inovadoras como machine learning, inteligência artificial (AI) e automação, indicando que há ainda mais terreno a conquistar com o aumento de investimento em inovações e soluções ciber resilientes.

CIBERSEGURANÇA:
UM CICLO DE PROTEÇÃO.

Num contexto de segurança exigente e com intervenientes muito inovadores, as empresas necessitam de garantir a segurança das suas redes. Um plano para mitigar falhas deverá por isso ser uma prioridade para o IT Manager, devendo ser também ele a assegurar o cumprimento desse plano e o ciclo de vida da estratégia de cibersegurança.



SÃO INGREDIENTES FUNDAMENTAIS NO PLANO DE QUALQUER ORGANIZAÇÃO QUE ESTEJA COMPROMETIDA COM A MELHORIA DA SUA POLÍTICA DE GESTÃO DE AMEAÇAS E ATAQUES. OS GESTORES DEVERÃO PROMOVER UMA ESTRATÉGIA DE INVESTIMENTO EM MECANISMOS DE PROTEÇÃO PROATIVA E PREVENÇÃO, E NÃO TANTO NA RECUPERAÇÃO DE INCIDENTES.

As empresas têm de:

- **Proteger os seus ativos físicos e a informação através de soluções de segurança.** Devem ter um plano de gestão de crise que inclua os vários passos para responder a um cenário de ameaça ou ataque. Neste alinhamento defensivo, o plano de disaster recovery também deve estar preparado para ser acionado de forma a dar respostas imediatas a eventuais ataques.
- **Identificar onde estão as suas vulnerabilidades e que recursos possuem para responder a ataques.** Os mecanismos de controlo e de gestão de riscos devem integrar uma política de segurança bem definida. A conformidade com o RGPD deve estar também assegurada.
- **Detetar as ocorrências de cibersegurança em tempo útil** e se possível antes destas acontecerem, implementando mecanismos de monitorização contínua que facilitem a deteção e o combate mais eficiente aos ataques.
- **Responder imediatamente perante eventos de cibersegurança,** limitando os efeitos do ataque e as perdas decorrentes.
- **Recuperar o mais rapidamente possível de um evento de segurança, minimizando o impacto sobre o negócio,** é uma prioridade para os responsáveis de segurança. Um plano de continuidade de negócio deve estar sempre preparado para ser executado.

VULNERABILIDADES ABREM AS PORTAS AOS CIBERCRIMINOSOS

AO MESMO TEMPO QUE DINAMIZOU OS NEGÓCIOS, A TECNOLOGIA TROUXE ÀS ORGANIZAÇÕES UM NÍVEL DE EXPOSIÇÃO NUNCA ANTES EXPERIENCIADO. UMA EXPOSIÇÃO QUE SE AGRAVA A CADA DIA, A CADA HORA, MINUTO OU SEGUNDO. AS AMEAÇAS SÃO EMINENTES E OS CIBERCRIMINOSOS ESTÃO À ESPREITA DA MELHOR OPORTUNIDADE PARA ATACAR. O IT MANAGER DEVE ESTAR ALERTA E TER TODOS OS RISCOS PREVISTOS, INOVANDO SEMPRE A SUA ESTRATÉGIA DE DEFESA, EXISTINDO PONTOS QUE DEVERÃO SER UMA REFERÊNCIA NA SUA AÇÃO:

RGPD

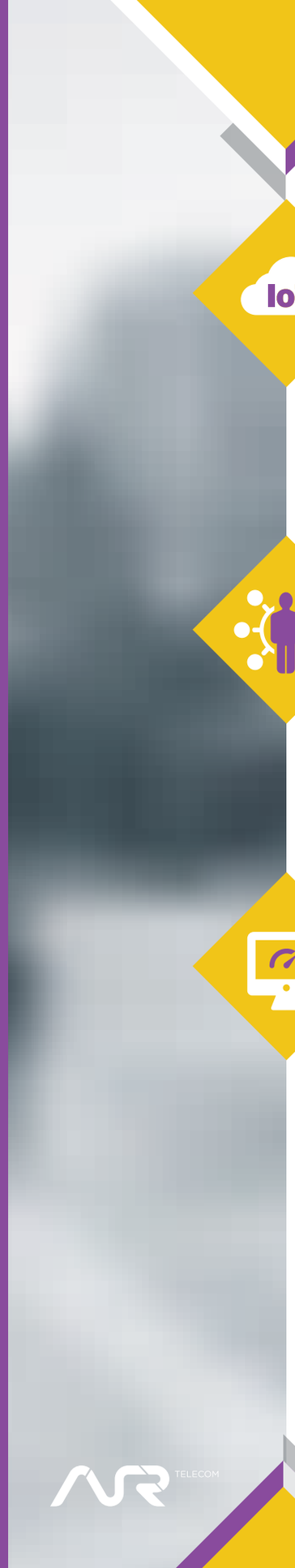
As empresas necessitam de garantir a confidencialidade, disponibilidade e integridade dos dados, bem como monitorizar, rastrear, auditar e apagar. O regulamento da União Europeia que entrou em vigor no passado mês de maio sublinha isso mesmo e estipula as elevadas multas que serão aplicadas às empresas que não assegurem este nível de proteção.

Inteligência artificial

A capacidade das máquinas aprenderem, à imagem do que acontece com os seres racionais, já está desenvolvida e começa a ganhar um lugar de destaque entre as soluções de gestão, mas não só. Na área de segurança, estas capacidades de machine learning são bem-vindas, já que permitirão prever de forma precisa os ataques e gerar rotinas de defesa automatizadas. No entanto, o risco destas tecnologias caírem do outro lado da barricada existe, e uma vez nas mãos dos cibercriminosos, serão igualmente poderosas.

Proatividade

Estar um passo à frente dos atacantes é sempre uma boa estratégia de jogo. O ransomware exige isso mesmo, que as organizações atuem na área da atualização dos seus sistemas, para que não sejam surpreendidas. Veja-se o que sucedeu no ano passado com o WannaCry. O impacto teria sido menor se esta proatividade fosse um "modus operandi" nas organizações e se os gestores estivessem munidos do know how adequado para agir de imediato.



IoT

A conectividade de todas as coisas, ou IoT, está a aumentar a exposição das redes e dos dispositivos, abrindo espaço para que a criatividade dos criminosos se desenvolva de uma forma sem precedentes. As organizações devem estar atentas a esta realidade porque a tendência é para que a IoT aumente a sua influência em todas as frentes e se não houver um alicerce de segurança bem estruturado, as possibilidades dos sistemas colapsarem perante ataques em massa são significativas.

Skills

Ter mecanismos de defesa é importante, mas ter as pessoas certas para os orquestrar e gerir vale ouro. Os profissionais de segurança escasseiam e é necessário que o setor da educação, mais concretamente as universidades e entidades de formação, agilizem ações nesta área para que a falha de recursos especializados seja colmatada e as empresas possam recrutar os CISOs de que necessitam para travar o tsunami de ataques que emerge com o mundo interconectado.

Desenvolver e testar

Para além da utilização de frameworks de segurança comuns, em que o contributo de muitos especialistas pode ajudar a inovar mais rapidamente as soluções de segurança e as estratégias de defesa das organizações, os gestores também devem perceber que ao testarem as suas políticas de segurança regularmente estarão a dar um grande passo para responder a um número considerável de vulnerabilidades de forma imediata e sem falhas. As políticas de segurança não se fazem para se guardar numa gaveta à espera do momento em que serão necessárias. Há todo um trabalho de desenvolvimento continuo que é necessário executar e testar para que nos cenários de risco as soluções e as equipas se articulem para responder às ameaças, minimizando o impacto dos ataques na organização.

TECNOLOGIA QUE PROTEGE O NEGÓCIO

Desenganem-se os que pensam que o cibercrime está controlado. Os criminosos estão em todo o lado e muitas vezes até integram as equipas das empresas. Ações imprudentes como clicar em links não autorizados, ou retirar dados de dispositivos de armazenamento não autorizados também é crime.

A TECNOLOGIA QUANDO USADA CORRETAMENTE, É UM FORTE ALIADO NA PROTEÇÃO E NA SEGURANÇA DAS ORGANIZAÇÕES:

Antivírus

É um software que deteta, impede e atua na remoção de programas de software maliciosos, como vírus e worms. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança aos utilizadores. Os gestores têm no antivírus um aliado de defesa de primeira linha, que os ajuda a evitar pesados danos para as organizações. Hoje é possível encontrar ferramentas à medida de todas as necessidades que permitem a defesa primária e a remoção de vírus e ransomware, bem como decifram os arquivos que foram atingidos num ataque. Para funcionar, este tipo de software deverá estar corretamente configurado e atualizado, pois só assim poderá identificar as ameaças mais recentes.

IDS / IPS

Sistemas de deteção de intrusão (IDS) ou sistemas de prevenção de intrusão (IPS) são reforços importantes quando o assunto é inspecionar o tráfego da rede em tempo real, procurando detetar vulnerabilidades ou ameaças. O IDS é uma ferramenta utilizada para monitorizar o tráfego da rede, detetar e prevenir eventuais ataques ou tentativas de acesso suspeitas, verificando de forma automática se este acesso ou comportamento é ou não uma ameaça. Por sua vez, o IPS é um mecanismo de segurança mais ativo, já que tem capacidade para identificar um ataque, analisar o risco e bloquear a ameaça para que ela não progrida na rede.

Firewall /UTM

A firewall é um dispositivo de segurança da rede que monitoriza o tráfego de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Ao longo dos tempos este dispositivo evoluíu para mecanismos de gestão de ameaças (UTM - Unified Threat Management), que centralizam numa plataforma única várias soluções de segurança, como:

- **Firewall;**
- **Filtragem stateful;**
- **VPN;**
- **Proxy web;**
- **Antivírus;**
- **IDS/IPS;**
- **Balanceadores de carga;**
- **Relatórios e logs;**
- **Inspeção profunda de pacote (DPI).**

A principal vantagem desta solução é a simplicidade, as organizações podem ter todas estas soluções de segurança sob o controle do mesmo fornecedor e executadas através de uma única consola de gestão.

SIEM

É uma solução para a gestão de correlação de eventos de segurança que permite às organizações identificarem e correlacionarem eventos de segurança em tempo real, de forma a preverem automaticamente comportamentos anormais e, desta forma, eliminarem rapidamente um ataque bem-sucedido. As soluções SIEM podem minimizar riscos detetando ataques em fases iniciais, que escapam aos "radares" de outras soluções de segurança.

Principais benefícios:

- **Garantia de elevados níveis de segurança nos ambientes protegidos**
- **Identificação e bloqueio, em tempo real, de ataques e ameaças**
- **Identificação ativa de fragilidades e riscos**

AMP / APT

Mais do que vigiar continuamente as redes, as soluções de proteção avançada contra malware (AMP) eliminam automaticamente todas as ameaças avançadas detetadas. A integração com as soluções de APT ou ameaças avançadas persistentes (APT), permite que as organizações acompanhem a evolução das ameaças a longo prazo, prevendo possíveis riscos e, desta forma, neutralizem os ataques direcionados que eventualmente poderão estar a ser preparados.

Encriptação de dados

Os mecanismos de encriptação permitem a transformação reversível da informação de forma a torná-la incompreensível por terceiros. A encriptação não previne que a informação seja acedida, mas impede que a mesma seja percebida, ou seja, através da encriptação garante-se que só terá acesso aos dados quem tiver legitimidade para os aceder.

Para proteger a informação e os dados dos seus funcionários, clientes e parceiros, as organizações devem incluir a encriptação de dados na sua estratégia de segurança. A força da encriptação está relacionada com a dimensão da chave (bits) e com o algoritmo utilizado. A forma mais simples de contornar a encriptação é experimentar todas as chaves possíveis. Este método é conhecido por ataque de brute-force, sendo que em muitos casos é ineficaz quando se trata de chaves de grande dimensão.

A encriptação normalmente é aplicada de duas formas distintas:

- **Armazenamento encriptado – é normalmente utilizada para encriptar na totalidade um disco ou um dispositivo. Este tipo de encriptação apenas se torna eficaz quando o sistema é parado, o disco ejetado ou a chave de encriptação bloqueada.**
- **Conteúdo encriptado – também conhecido por encriptação granular – significa que os ficheiros ou o texto são encriptados ao nível da aplicação. O exemplo mais comum é a encriptação por email, onde o formato da mensagem deve permanecer intacto para a aplicação de email cliente ser capaz de lidar com a mesma, mas o corpo da mensagem permanecer encriptado, bem como todos os anexos.**

Encriptar e o RGPD?
Um dos princípios fundamentais do RGPD é assegurar a proteção eficaz dos dados pessoais. A encriptação é uma medida técnica adequada para alcançar este objetivo, já que ao encriptar os dados pessoais que armazenam as empresas passam a estar totalmente protegidas no caso de uma fuga de informação, garantindo o cumprimento do regulamento.

FORMAÇÃO CONTÍNUA

Os colaboradores são o elo mais fraco em todo o sistema de cibersegurança. A formação em segurança é um must-have em todas as empresas. A mais pequena distração pode dar origem a uma falha de segurança grave. A estratégia de segurança deve ter este ponto em atenção e não deixar para depois a formação dos seus recursos internos, que deverão estar conscientes do que devem e não devem fazer perante os seus equipamentos de trabalho.

O investimento em formação é essencial para o sucesso de qualquer política de segurança e deve ser realizada não só na teoria, mas também na prática, no posto de trabalho.

Também aqui os IT Managers deverão saber identificar se possuem internamente todas as competências necessárias para formar condignamente as suas equipas ou recorrer a um parceiro externo que assegure a consultadoria nesta área e faça o assessment e auditoria, com base na qual serão definidas: plataformas tecnológicas, processos de gestão e operação, planos de mitigação e de gestão de crise.

CONCLUSÃO

ANTIVÍRUS, MALWARE REMOVERS, PATCHS DE SEGURANÇA, FIREWALLS, SISTEMAS DE DETEÇÃO DE INTRUSÕES SÃO TODOS TERMOS QUE OS IT MANAGERS TÃO BEM CONHECEM. UNS PORQUE JÁ LHES CAUSARAM INÚMERAS DORES DE CABEÇA, OUTROS PORQUE FORAM O REMÉDIO SANTO PARA A DOR. O CERTO É QUE A ESTES VÃO-SE JUNTANDO MUITOS OUTROS, ALGUNS COM NOMES IMPRONUNCIÁVEIS. O PARADIGMA DA SEGURANÇA ESTÁ A MUDAR EMPURRADO PELA INOVAÇÃO TECNOLÓGICA QUE NÃO CONHECE LIMITES. À MEDIDA QUE SE DESENVOLVEM NOVOS SISTEMAS E SE LIGA O MUNDO EM REDE, OS CIBERCRIMINOSOS TAMBÉM VÃO INOVANDO OS SEUS MECANISMOS DE ATAQUE, IDENTIFICANDO AS FALHAS QUE OS EMPREENDEDORES DO FUTURO VÃO DEIXANDO PARA TRÁS.

É por isso que as organizações não se podem distrair daquilo que são os princípios de segurança fundamentais e devem atualizar as suas políticas de segurança em conformidade com as últimas regras, leis ou regulamentos. O RGPD deve servir como farol para conduzir as estratégias de segurança e mostrar que correr riscos não compensa e pode trazer perdas incalculáveis.

A monitorização contínua, a reavaliação periódica dos riscos e a eficácia das decisões tomadas são ações que devem estar diariamente na agenda dos IT Managers. As empresas devem definir a melhor estratégia de defesa, quer esta seja assegurada internamente ou por um parceiro especializado que dê garantias de tranquilidade, de forma a permitir aos gestores concentrarem-se no negócio, na sua estratégia e no seu crescimento.

SOBRE A AR TELECOM

NASCEMOS HÁ 18 ANOS DA AMBIÇÃO DE TRANSFORMAR O SETOR DAS COMUNICAÇÕES EM PORTUGAL

SOMOS UMA EMPRESA SÓLIDA, AUTÓNOMA, RESPONSÁVEL, ORIENTADA PARA O CLIENTE E COMPROMETIDA COM O INVESTIMENTO CONTÍNUO EM NOVAS SOLUÇÕES. MERECEMOS A CONFIANÇA DOS NOSSOS CLIENTES, AOS QUAIS DEDICAMOS UMA LEALDADE INCONDICIONAL QUE SE REFLETE NA SUA SATISFAÇÃO E FIDELIDADE.

DISPONIBILIZAMOS UMA OFERTA COMPLETA DE SOLUÇÕES CLOUD E MANAGED SERVICES, PARA QUE O DEPARTAMENTO DE TI DE CADA EMPRESA SE DEDIQUE A PROJETOS ESTRATÉGICOS E QUE EXIGEM RECURSOS FOCADOS E DEDICADOS.

O CONHECIMENTO DAS ESPECIFICIDADES DE CADA SETOR DE ATIVIDADE, PARA MELHOR ADEQUAR AS SOLUÇÕES ÀS NECESSIDADES DE CADA CLIENTE, É UMA DAS GARANTIAS DADAS PELA AR TELECOM.

PRECISA DE AJUDA? ENTRE EM CONTACTO CONNOSCO!