Segurança: Um Novo Paradigma

Um crescente número de ciberataques à escala global está a colocar a segurança no topo da agenda internacional. O desenvolvimento tecnológico, a previsão do aumento de ameaças e a crise económica obrigam a novas medidas de defesa no ciberespaço e fora dele. A colaboração aumenta

Sónia Gomes da Silva

O Forum Económico Mundial (FEM), vários governos, consultoras, empresas e investigadores em todo o mundo estão a redobrar esforços para desenvolver novas medidas de segurança que mitiguem os prejuízos causados por ataques no ciberespaço a organizações comerciais e governamentais. O grande alerta decorre de uma série de ataques ocorridos ao longo do ano de 2014.

A consultora PwC, no estudo de segurança da informação "Ciber-riscos: Um Perigo Presente e Severo" diz que "quase todos os sectores de atividade foram afetados nos últimos 12 meses. No retalho (norte-americano), os ataques atingiram níveis épicos, resultando no roubo de centenas de milhões de cartões bancários, impulsionando os EUA a adotar um novo standard para os cartões de pagamento". Acresce-se a revelação da vigilância no ciberespaço de indivíduos, negócios e nações, do qual o caso Snowden é um exemplo, e casos de espionagem como os revelados pela Symantec, que descobriu a existência de ataques contra governos europeus durante pelo menos quatro anos, através do Regin - um software malicioso que tem espiado indivíduos, governos, investigadores, empresas, telecomunicações e infraestruturas e que terá sido usado primeiro na Rússia, na Arábia Saudita, e em países como o Afeganistão, Áustria, Bélgica, Índia, Irlanda, México e Paquistão.

O desacordo entre a Russia e a Ucrânia resultou em ciberataques entre ambas as nações, deitando abaixo websites governamentais e disseminando malware nos computadores das embaixadas. Os sistemas de controlo de centenas de empresas de energia na Europa e nos EUA foram atacados com malware sofisticado. O Heartbleed afectou dois terços dos servidores web do mundo, acreditando-se que tenha comprometido milhões de websites, lojas online, aplicações de segurança, software como o instant messaging, ferramentas de acesso remoto e dispositivos de rede. Uma cadeia hospitalar norte-americana anunciou o roubo de 4,5 milhões de dados clínicos de pacientes em Agosto. Os ataques ao banco JP Morgan, ao eBay, à Sony Pictures, que ficou paralisada durante uma semana, entre outras empresas de média e grande dimensão, colocaram em causa a sua reputação, gerando prejuízos de elevada gravidade.

Em 2014 houve ainda ataques a dispositivos dos consumidores, como televisões, monitorizadores de bébés e termóstatos, comprometendo o desenvolvimento da Internet das Coisas (IoT), devido à falta de segurança em muitos destes dispositivos. Também os media foram alvo de ataques no ciberespaço, como o New York Times, o The Financial Times, a CNN e a Reuters. No Reino Unido foi roubada informação de 100 mil empregados de uma cadeia de supermercados e publicada online. A lista de ataques internacionais em 2014, à escala mundial, é exaustiva.

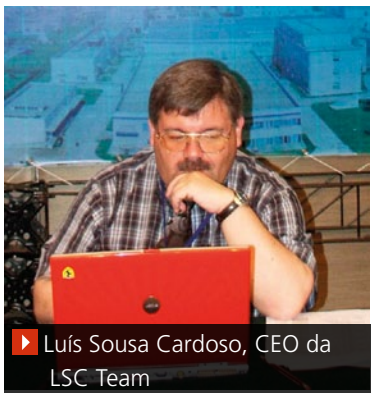
Em Portugal

O recente estudo "Security Intelligence nas Organizações Nacionais", realizado pela IDC em Portugal com o apoio da Mainroad, empresa do grupo NOS,

também assinala a multiplicação de ataques em território nacional. "O grupo Anonymous reivindicou uma série de ataques contra sites de organismos públicos – divulgando nomes e números de telemóveis dos procuradores públicos - e de entidades privadas – EDP, BES, Barclays e Banif foram alguns dos sites atacados por esta organização, enquanto foram divulgados na imprensa os primeiros casos de extorsão online no território nacional", lê-se no documento. A empresa diz que os ataques resultam do "efeito conjugado da emergência da Terceira Plataforma tecnológica de inovação das tecnologias de informação, assente nos serviços de cloud computing, mobilidade, social business e soluções de big data e analítica de negócio", e que a "crescente sofisticação das ameaças à segurança da informação veio alterar significativamente as condições de gestão da segurança da informação no interior das organizações a nível mundial, assim como lançar novos desafios aos seus responsáveis. No território nacional, a recessão das atividades económicas nos últimos anos veio agravar esta realidade".

Se, por um lado, se assiste ao aumento do investimento em segurança a nível internacional, com a empresa de estudos de mercado Gartner a indicar um aumento de 7,9%, cerca de $71.1 mil milhões no ano 2014, e novo aumento de 8,2% em 2015, na ordem dos $76,9 mil milhões, por outro lado a crise económica impede o reforço da segurança de muitas empresas em Portugal. Segundo a IDC, "neste contexto, não será de estranhar que, apesar do grau de risco das organizações ser negativo, o mesmo aumentou nas organizações nacionais nos últimos anos. Os dados compilados permitem constatar que, num espaço de dois anos, o grau de risco das organizações nacionais cresceu. E esta alteração é particularmente visível nas ameaças relacionadas com phishing, vírus/worms, spyware, spam, passwords e ataques a websites".

O problema maior nas telecomunicações "é a entrada dos smartphones, especialmente os Androids, que são completamente vulneráveis e, na prática, quando as empresas de telecomunicações o permitem, estão a ligar os Androids através do IP à própria rede. A partir de um Android tenho acesso à rede da empresa e é fácil identificar a quantidade de malware que se espalha", explica Luís Sousa Cardoso, CEO da LSC Team, questionando "quantas pessoas sabem usar ou proteger o seu smartphone? E o mesmo se passa a nível mundial. Carregam todo o tipo de aplicações e depois têm problemas. Através de uma aplicação dessas, com bonecos, que as pessoas acham muito engraçadas, chega-se às redes das organizações", tornando os utilizadores em veículos para novas formas de engenharia social.



Luís Sousa Cardoso, CEO da LSC Team

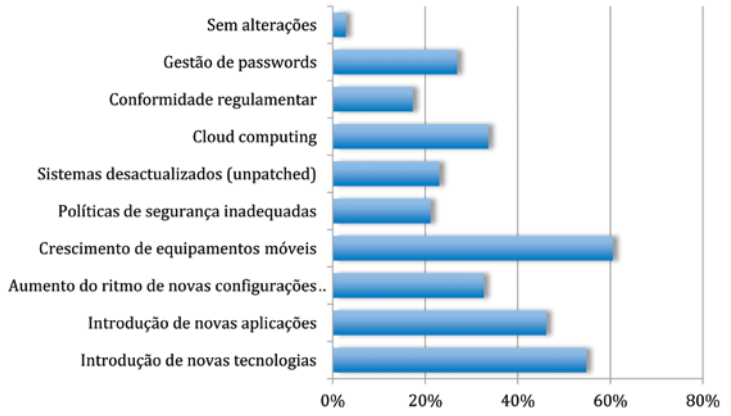
"Quem está a realizar ataques desta dimensão são exércitos, que fazem parte da guerra do ciberespaço. Não são hackers individuais, esses são muito poucos neste momento"

Soluções

Perante a falta de maturidade na área da segurança por parte das organizações nacionais, que também é assinalada pela IDC, Sousa Cardoso, responsável por trabalhos em curso na área da segurança das redes nos Emiratos Árabes Unidos, Zimbabwe e Cabo Verde, e consultor da SATA (Southern Africa Telecommunications Association), sugere que as empresas façam gestão de risco do valor da informação que têm, um levantamento dos bens e que, depois, decidam como querem proteger-se. Diz que, como as empresas portuguesas estão descapitalizadas, a solução passa "muito pelo investemento na cloud, onde é possível concentrar especialistas para fazer a proteção de dados, transferindo a responsabilidade da segurança através de contratos. O problema é quando os ataques são feitos na cloud, a informação perdida é muito maior".

Com as organizações sujeitas a maiores penalidades financeiras, a um maior escrutínio regulatório, a um estrago reputacional tangível e com a impossibilidade de garantirem níveis de segurança elevados, para as que sofrem incidentes, Steve Durbin, Managing Director do Information Security Forum, diz que se devem preparar para responder de forma "confiante e inteligente. A verdadeira dificuldade assenta em reconhecer que a violação de dados é inevitável e que os recursos investidos na prevenção podem trazer dividendos quando as crises

Fatores que mais contribuíram para uma maior complexidade da gestão da Segurança da Informação nas organizações inquiridas



Fonte: IDC, 2014

ocorrem. É preciso maturidade para que uma organização reconheça que não consegue controlar uma narrativa depois dos ataques se tornarem públicos e que a liderança envolve ser honesto e transparente com os clientes para manter a credibilidade em circunstâncias difíceis".

A resposta a um ataque robusto começa na prevenção. Inclui desenvolver um plano, tomar ações decisivas e gerir a mensagem. Estas ações envolvem "um vasto número de profissionais internamente, e pode envolver os serviços de uma crise de gestão externa e de especialistas de media. Uma vez ocorrido o ataque, é necessária a obtenção de dados precisos para rápidas tomadas de decisão. Para aqueles que têm a responsabilidade última de lidar com a violação de dados – o Chief Information Security Officer (CISO) ou equivalente -, o primeiro desafio é estabelecer expetativas e a credibilidade, o que acontece através de ações claras, quer nos momentos fáceis ou difíceis".

Enquanto a Internet das Coisas estiver na sua infância, existe a possibilidade de construir novas abordagens de segurança "se nos começarmos a preparar desde já. As equipas de segurança devem, então, tomar a iniciativa de pesquisar as melhores práticas para assegurar estes dispositivos emergentes e prepararem-se para atualizar as políticas de segurança consoante o número de dispositivos interligados a entrar nas redes das empresas. As organizações com o conhecimento apropriado, liderança, políticas e estratégias no lugar, ficam mais ágeis para responder a lapsos de segurança inevitáveis".

Durbin afirma que as organizações produtoras de respostas credíveis e criativas vão certamente ganhar vantagem sobre as que forem lentas e confusas e isso vai traduzir-se no valor tangível do negócio. Com a velocidade e complexidade da paisagem de ameaças a mudar numa base diária, o diretor acredita, tal como outros profissionais do sector, que "vamos ver negócios perdidos com frequência" e aconselha as organizações a precaverem-se já para garantir que estão completamente preparadas e comprometidas para lidar com os novos desafios de segurança, antes que seja tarde demais.

Passos na Gestão de Risco

O governo britânico, através das empresas HSB e Trail of Bits, disponibilizou recentemente dicas essenciais para a gestão de risco de pequenas empresas, mas que também servem o utilizador final e as redes domésticas. Para evitar que as informações bancárias sejam comprometidas, recomenda que as empresas usem um computador específico para as transações financeiras online e um dispositivo diferente para o e-mail e o social media. Nunca usar as mesmas passwords

Steve Durbin, Managing Director do Information Security Forum

"É preciso maturidade para que uma organização reconheça que não consegue controlar uma narrativa depois dos ataques se tornarem públicos"

e nunca confiar na funcionalidade oferecida pelos websites para as guardar, pois nunca se sabe se esse website já foi 'hackado', podendo nesse momento os criminosos estar no processo de recolha de informações, como aconteceu com a Sony Pictures, cujo ataque teve início em Setembro e a recolha de dados decorreu até Dezembro.

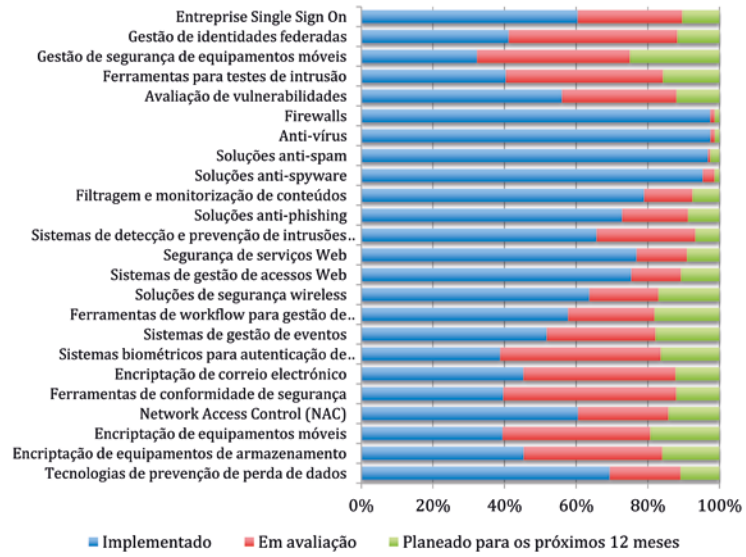
Criar por escrito e implementar políticas para a segurança de dados, comunicá-la a todos os funcionários, explicando que tipo de informações são confidenciais ou mais sensíveis e quais as suas responsabilidades sobre esses pedaços de informação, independentemente de serem grandes ou pequenos. Como a maior parte dos esquemas e ataques maliciosos chegam por e-mail, é necessário ensinar a identificar os e-mails que podem ser suspeitos e, uma vez detetados, os colaboradores devem alertar os colegas dentro da organização.

Manter-se informado, monitorizando toda a cadeia de acontecimentos num possível ataque às infraestruturas tecnológicas da empresa. Do e-mail à vulnerabilidade do browser, é essencial identificar qual a área que está mais em risco dentro da empresa e questionar a postura de políticas de segurança de toda a linha de negócio, dos fornecedores aos parceiros de negócio.

Garantir que todos os dados da empresa são encriptados, quer estejam em arquivo ou em movimento, assim como todos os e-mails da organização que contenham dados pessoais, evitar usar redes Wi-fi e manter os browsers atualizados com as últimas versões. Usar sempre as versões mais recentes dos sistemas operativos, porque as antigas deixam de ser atualizadas pelos fornecedores, o que potencia a entrada de intrusos no sistema.

Ter uma password de administração forte no router e nas ligações Wi-Fi pode ser vital para evitar possíveis interceções. Fazer backups encriptados e mantê-los noutra localização é essencial, pois se a empresa sofrer um ataque, acidente ou o equipamento for roubado, consegue mais facilmente dar continuidade ao negócio.

Mecanismos de controlo de segurança de informação



Fonte: IDC, 2014

O FEM, em parceria com a Deloitte, apresentou recentemente o relatório "Partnering for Cyber Resilience Towards the Quantification of Cyber Threats" (http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf), que visa facilitar que as empresas a realizem a sua própria gestão de risco, apresentando um método de análise e criação de soluções. A empresa deverá fazer um levantamento das ameaças a que pode estar sujeita, identificando as suas diversas origens, como o hacktivismo, a espionagem empresarial, o terrorismo. De seguida deve enumerar as vulnerabilidades existentes, que podem ser acidentais ou derivar da falta de boas práticas, quer em relação às tecnologias adoptadas, aos processos do negócio ou às pessoas. Na sequência do levantamento destes dados, o FEM e a Deloitte dizem ser possível fazer uma correcta avaliação do risco, tendo em conta os bens e a reputação da empresa. A partir desse ponto, deve desenvolver respostas de acordo com as regulamentações e as políticas em vigor.

Que desafios trará a IoT?

"Com a IoT, os paradigmas de segurança desenvolvidos nos últimos 25 anos deixam de ser válidos e vão mudar cada vez mais. Um dos grandes problemas é a perda do perímetro de segurança. Costumávamos protegê-lo com ferramentas que todos conhecem, como a firewall, mas com a IoT e em particular os dispositivos móveis, o perímetro torna-se muito dificil de estabelecer", explica Carlos Ribeiro, pró-reitor na Universidade de Lisboa, professor no IST e investigador no INESC. "Imagine-se a quantidade de objetos que vão ser atualizados. E como isso se vai proceder, ainda é algo que nos ultrapassa".

Além do problema da privacidade, "a inferência resultante da quantidade de informação torna-se num grande problema que tem de ser endereçado. Não é bem um mundo novo, mas é o mundo atual multiplicado, com um efeito de escala muito relevante e a capacidade de inferência de um atacante depende da quantidade de dados que tem. Ainda não percebemos muito bem o que é que essa escala faz às coisas".

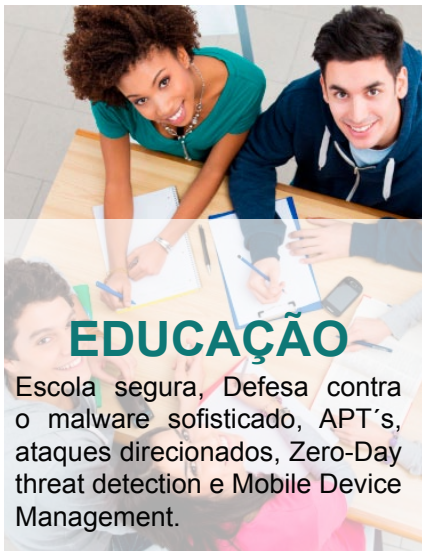
Do ponto de vista da segurança das empresas, o investigador adianta que "é muito complicado, porque já têm de resolver o BYOD e vão passar a ter de se preocupar com múltiplos dispositivos. Têm de estar preparadas para os gerir, o que implica um esforço muito maior dos departamentos de informática e um aumento de investimento em ferramentas e conhecimento".

O engenheiro Luís de Sousa Cardoso diz ser fundamental o investimento dos fornecedores desta tecnologia na educação dos utilizadores. "Agora a segurança é mais crítica porque toda a sua filosofia está a ser alterada. Se as pessoas compravam equipamentos e se baseavam na segurança feita pela rede de telecomunicações, agora o paradigma mudou e a segurança tem de ser concretizada no desenvolvimento das aplicações. Tal como nos telemóveis, os problemas advêm do spyware e esse reside nas aplicações e não das redes de telecomunicações".

Carlos Ribeiro, professor no IST, investigador no INESC

A par dos riscos já enunciados, este diretor acrescenta as vulnerabilidades decorrentes dos novos tipos de redes wireless, como sejam os pequenos operadores, redes comunitárias e operadores celulares em spectrum partilhado, para comunicações pessoais, redes mesh, redes ad hoc híbridas, ou "multi-hop cellular networks", as redes ad hoc autónomas, as redes de área pessoal, redes RFID, de sensores e de viaturas automóveis. Nestas enquadram-se rádios cognitivos, MIMO, a ultra wide band e as antenas direcionadas.

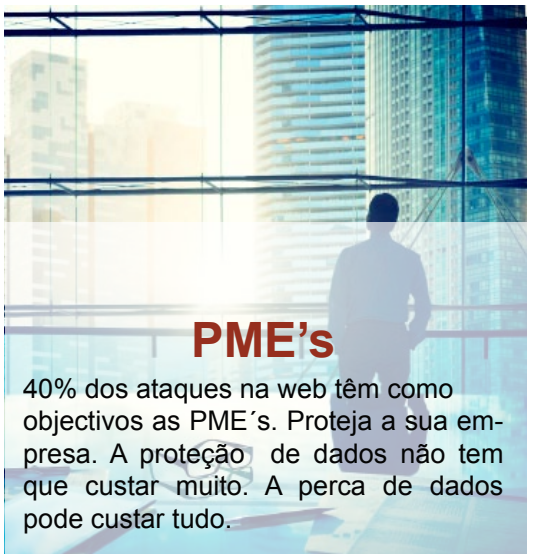
Sousa Cardoso levanta maiores preocupações nas aplicações que venham a ser desenvolvidas nos campos da saúde, em meios hospitalares e na vida rodoviária, onde os hackers podem constituir maior problema.



EDUCAÇÃO

Escola segura, Defesa contra o malware sofisticado, APT´s, ataques direcionados, Zero-Day threat detection e Mobile Device Management.

Proteja a informação e os sistemas que mantêm a sua empresa a funcionar localmente, virtual e na cloud com as tecnologias mais seguras.



PME's

40% dos ataques na web têm como objectivos as PME´s. Proteja a sua empresa. A proteção de dados não tem que custar muito. A perca de dados pode custar tudo.

SEGURANÇA EMPRESARIAL COM TECNOLOGIAS AVANÇADAS

As Soluções que necessita para proteger a sua empresa: Segurança Física, Virtual e Cloud.

LOGÍSTICA

O desafio para uma empresa de logistica é conseguir melhorar os seus prazos de entrega. As nossas Soluções de Mobilidade e Segurança premitem intervir em tempo real.

SETOR FINANCEIRO

Proteger a confidencialidade dos documentos é fundamental, bem como não divulgar informações inadequadas intencionalmente ou por erro.

SAÚDE

Proteger os doentes protegendo o IT. Backup e recuperação instantânea.

SETOR PÚBLICO

Confidencialidade e rapidez são problemas do sistema judicial. Conheça as soluções de segurança e backup de dados nesta área.

- BACKUP & RECOVERY
- ANÁLISE DE RISCO
- MOBILIDADE AUTENTICAÇÃO
- SEGURANÇA ENDPOINT
- DATA LOSS PREVENTION
- WEB MONITORING

minitel
28 anos a distribuir valor

info@minitel.pt | +351 21 381 09 00
www.minitel.pt

Symantec. LACIE SEAGATE QNAP crucial ThreatTrack Security SOTI

DeviceLock Proactive Endpoint Security UNITRENDS Unified Data Protection, Without Limits VIPRE SpectorSoft LabTech

TENDÊNCIAS PARA 2015: mudanças na segurança empresarial, diferentes tecnologias para cada setor de atividade

João Fonseca George, Diretor de Estratégia da Minitel

O ano de 2014 assistiu à ascensão do que conhecemos como “Big Data”, com as organizações a quererem retirar benefícios diretos para a sua atividade através da análise dos dados dos seus negócios, precisando para tal de guardar esses dados de forma segura e com acesso fácil. O expectável aumento desta tendência em 2015 irá implicar mudanças na segurança empresarial, já que o número de ataques aos sistemas de armazenamento da informação, por norma vulneráveis, aumentou em 2014 na razão directa do crescimento desses sistemas.

Assim, em 2015, iremos assistir a modificações no paradigma da segurança empresarial, até aqui centrada na proteção da rede e dos postos de trabalho. Existem hoje diferentes tipos de segurança, End Point Security (a mais clássica), Data Security, Data Leak Security ou Enterprise Network Security, cada uma das quais protege diferentes pontos de ameaça. A segurança tornou-se mais especializada, mais personalizada por organização, tornando-se claro para as empresas que têm de investir em novas tecnologias de segurança.

Portfólio da Minitel

Há 28 anos no mercado português, a Minitel sempre teve como missão de trazer às empresas portuguesas as melhores soluções para as necessidades de cada negócio e, mais uma vez, preparámo-nos para estas mudanças. Construímos assim um portfolio de soluções avançadas capazes de servir qualquer área de negócio, e prontas para serem implementadas em qualquer sector ou atividade, o que nos confere uma abrangência nas zonas de **Enterprise Security, Endpoint Security , Data Security , Mobility, Análise de Risco ,Web Monitoring , Data Loss Prevention , Disaster Recovery, Enterprise Backup, Storage e Remote Monitoring Management.**

Diferentes tecnologias para cada setor de atividade

Este portfólio é importante já que a evolução das estruturas de armazenamento de dados e das estruturas de segurança, aliados aos desenvolvimentos em mobilidade, cloud, wireless, big data e virtualização, implica diversas possibilidades para as empresas conforme a sua actividade (algo que nem sempre aconteceu no passado) sendo por isso importante fazer as escolhas certas.

Uma dessas escolhas é por exemplo a segurança base da empresa, Endpoint Security. Durante anos aceitaram-se atrasos nos sistemas e reduções na produtividade dos colaboradores, mas na economia global, é cada vez mais importante que a produtividade no trabalho seja elevada. Por essa razão, o **VIPRE** é uma solução interessante. Para além de ser a primeira solução antivírus a oferecer uma gestão de segurança integrada para Microsoft Windows Server Hyper-V, a sua forma de gestão e pesquisa a partir do servidor permite uma tecnologia de deteção de ameaças avançada, sem que isso implique a degradação de performance nos diferentes postos de trabalho característica noutras soluções. Também neste campo torna-se vital para as empresas entenderem a origem das suas perdas de produtividade. A **SpectorSoft** traz-nos uma inteligente solução de Web Monitoring, que permite definir politicas de alerta e resposta a diferentes comportamentos, de forma a manter os colaboradores focados no seu trabalho.

Outra das escolhas que as empresas terão de fazer tem a haver com o grande volume de informação com que têm lidar diáriamente, para não perderem a visibilidade do que está a acontecer com as suas redes e utilizadores (se não conseguirem ver, não conseguem reparar). A análise de riscos deve ser uma prioridade. A **Threat Track** disponibiliza ferramentas de gestão de risco através de uma sandbox pública, suportadas por processos de inteligência e análise de risco, permitindo uma abordagem e um enfoque preventivo da segurança e uma visibilidade que permite a identificação, análise e eliminação de cada ameaça.

E porque as organizações dependem das pessoas que delas fazem parte, será também importante que as empresas sejam capazes de reter a sua informação confidencial dentro de portas. Todos os dias assistimos a casos de fugas de informação, sejam estas informação financeira de empresas e operações a ser usadas por concorrentes, informações sobre processos jurídicos, ou informações sobre dados bancários divulgadas através das redes sociais ou imprensa. Com um grau de exigência modesto ao nível dos recursos necessários ao seu funcionamento e o leque de opções mais abrangente do mercado, o **DeviceLock** é sem dúvida a melhor solução para proteger as empresas contra a fuga de informação confidencial.

O ponto a reter sobre segurança é que a proteção de dados das empresas é fundamental e não tem de necessáriamente custar muito dinheiro, como se pensa. Por outro lado, um ataque bem colocado ou uma fuga de dados em massa pode custar ás empresas tudo o que têm. Estudos mostram que cerca de 60% das pequenas empresas que são vítimas destes ataques podem fechar num período de 6 meses. Felizmente, é possível proteger as organizações em qualquer área de atividade, de forma fácil e económica, combinando soluções de segurança com soluções de armazenamento e recuperação de dados, por exemplo, como temos na Minitel.
A crise levou a um mercado muito mais dinâmico, obrigando as empresas a tornarem-se mais rápidas e eficientes para continuarem competitivas. Assim, os dispositivos móveis tais como smartphones ou os tablets irão continuar a proliferar nos ambientes profissionais e pessoais do mundo atual. Faz assim sentido para uma seguradora, por exemplo, cujos peritos têm de obter e enviar informação, a necessidade de os equipar com tablets para melhor conseguir servir os seus clientes, ou que companhias de logística disponibilizem aos seus operadores smartphones para saberem o estado das cargas em tempo real. É fundamental implementar estratégias seguras ao nível da mobilidade, já que ter estes aparelhos de nada serve se não se conseguir gerir a informação produzida pelos mesmos.

A **SOTI** é um lider mundial em Soluções de Gestão de Dispositivos Móveis, com milhões de dispositivos geridos no mundo inteiro. A solução Mobile Device Management Mobi Control da **SOTI** faz a gestão do acesso a recursos empresariais, permitindo às organizações suportarem estratégias de Bring Your Own Device (BYOD), resolvendo desafios únicos de gestão, segurança, suporte e controlo de dispositivos móveis em diversas plataformas. Permite visualizar de uma forma global a rede e os diversos dispositivos móveis, de forma a gerir custos e automatizar a gestão a nível de mobilidade da empresa, aumentando a produtividade e forçando os procedimentos a adoptar a nível de segurança. Permite ainda aos gestores do sistema distribuir, gerir, actualizar e segurar aplicações em smartphones e tablets pessoais, da empresa ou partilhados.

Importância da proteção e soluções modernas de proteção de dados para PME´s

As empresas grandes têm especialistas dedicados e preparados para emergências caso ocorra um problema de dados, mas as organizações de pequeno e médio porte não tem esta opção. No entanto as PMEs podem adotar determinadas estratégias que as ajudem a tornarem-se mais eficazes no que respeita à protecção de dados. Por exemplo, podem olhar para tecnologias como as que são oferecidas pela Unitrends– soluções fáceis de adquirir e de implementar onsite, como appliances fisicas ou virtuais, e potencializar a cloud para uma protecção completa.

Casos de sucesso em logística /distribuição, educação e outros.

A **SOTI**, através de ferramentas avançadas a nível de segurança e controlo remoto, faz a gestão de cerca de 4000 dispositivos da empresa American Airlines, que utiliza com sucesso o MobiControl para ajudar a gerir e a manter os protocolos de segurança da sua rede.

As instituições de ensino enfrentam também inumeros desafiosde TI, do ensino básico e secundário até ao universitário. Estes desafios incluem desde a proteção de informações confidenciais em laptops, desktops e dispositivos móveis dos alunos, até ao controlo de acesso à rede e opções de salvaguarda dos dados. Além disso, as instituições de ensino necessitam de uma abordagem segura e económica para migrações e ensino à distância. O abrangente portfolio de soluções da Minitel proporciona a estas um ambiente de ensino seguro e controlado. Para além disso as escolas, colégios e universidades debatem-se com orçamentos reduzidos face a uma explosão do número de dispositivos móveis, utilizadores sem grandes conhecimentos, máquinas infectadas, software descactualizado e muito mais. O desafio de oferecer aos alunos o acesso às mais recentes tecnologias e ao mesmo tempo manter as redes seguras é a realidade diária. Desde a proteção endpoint até à defesa contra malware avançado – como APT´s , ataques direccionados ou zero-day, o **Threat TrackSecurity** tem as soluções necessárias contra estas ameaças .
A Minitel recomenda a Soti para uma solução abrangente de gestão de dispositivos móveis oferecendo mobile security, gestão de dispositivos, gestão de aplicações, gestão de conteudos segura, e integração móvel avançada.Com o MobiControl da Soti os professores podem automatizar a configuração dos dispositivos, implementar apps, distribuir de uma forma segura e atualizada.