Deloitte.

COVID-19

Keep safe during home office

Abril 2020

Home office: como podem as organizações reagir ao risco acrescido?

Assistimos nas últimas semanas a uma alteração massiva na forma de aceder aos ativos das organizações. Esta nova forma de trabalhar coloca as organizações mais expostas a ameaças cibernéticas. Enunciamos por isso um conjunto de pontos que julgamos críticos e que devem ser tidos em consideração.

Enfrentamos um período alargado em que os colaboradores estarão a trabalhar de forma remota. Cremos também que esta forma de trabalho passará a fazer parte do quotidiano das organizações de forma bastante mais acentuada do que até há algum tempo atrás.

No seu processo de preparação rápida para este plano de contingência as organizações poderão, em muitos casos, ter saltado alguns passos na segurança.

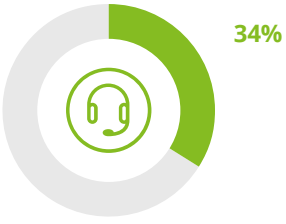
Convém hoje, olhar para trás e rever o que foi feito, preparando um futuro sustentável sem descurar a segurança.

Nos próximos tempos a superfície de ataque tecnológica e humana é imensamente superior: mais acessos remotos e mais equipamentos (geridos e não geridos) a aceder a recursos corporativos utilizando muitos deles redes e pontos de acesso inseguros. O distanciamento e a pressão para manter os mesmos níveis de rendimento leva a que muitos utilizadores, de forma isolada aumentem os níveis de clicking descuidado.

Agudizando a situação, os nossos Centros de Operações de Segurança reportaram nos últimos dias um aumento significativo de ataques específicos com informação sobre o COVID-19 pelos vários canais (ex.: email, SMS, navegação, entre outros).

Os atores internos foram no ano de 2019 uma das principais ameaças, nomeadamente por comportamentos negligentes. Prevemos que pelo seu isolamento, distanciamento e falta de linhas de comunicação direta com as equipas de segurança, estes utilizadores venham a representar um nível mais elevado de ameaça para as organizações.

Envolvimento de atores internos em fugas de informação em 2019 (%)[1]



Fonte: Verizon 2019 Data Breach Investigations Report

As organizações asseguram o mesmo nível de proteção dos equipamentos dentro e fora das suas redes?

Um dos pontos de maior criticidade neste contexto é assegurar a proteção de todos os equipamentos em utilização, em especial quando estão fora das redes corporativas e estas não estão devidamente preparadas para este contexto.

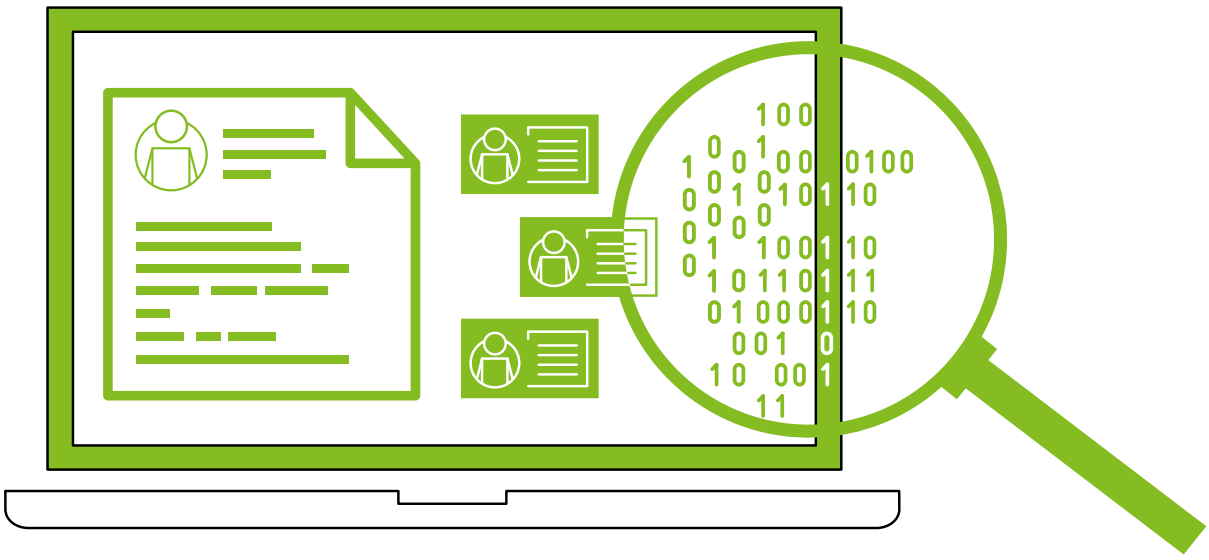
De que forma e com que periodicidade são asseguradas as atualizações de sistemas operativos e software corporativo nestes equipamentos? A forma mais fácil de operacionalizar esta atualização é garantir que os equipamentos são geridos pela organização, independentemente da sua localização. As atualizações devem ser despoletadas a partir de ferramentas que façam a gestão destes equipamentos, garantindo a obrigatoriedade da sua instalação e atualização dentro ou fora das tradicionais redes corporativas.

Não facilite.
As organizações estão agora mais expostas e vulneráveis porque muitas das suas políticas de segurança não estão a ser aplicadas fora da rede corporativa.

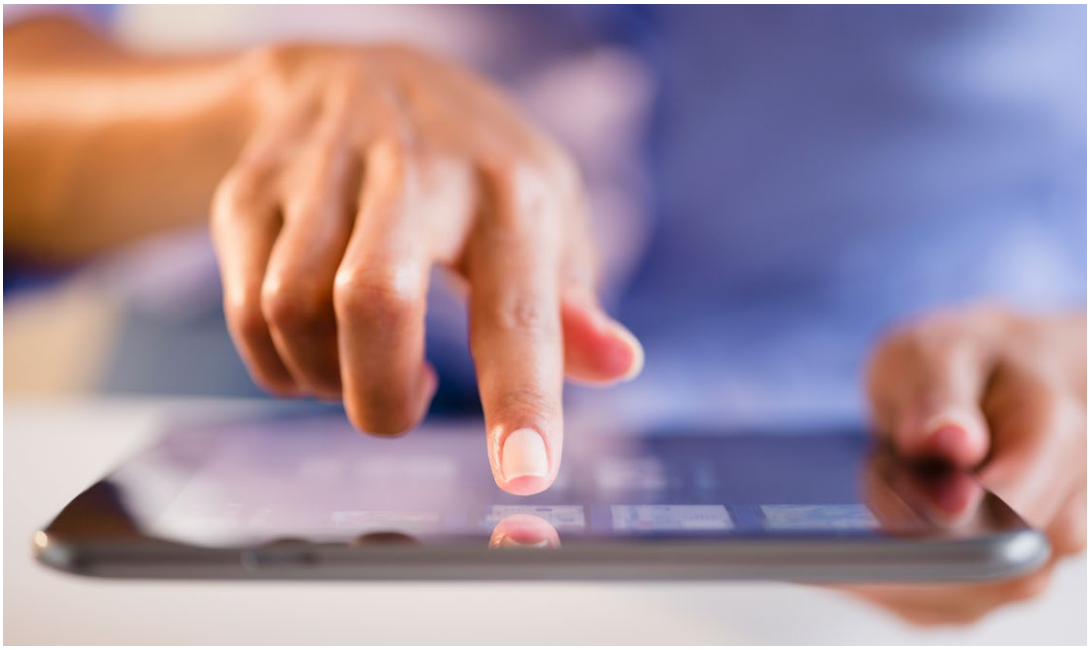
O acesso à internet é assegurado de forma controlada e similar à que é efetuada dentro da rede corporativa?

Em muitos casos este acesso fora da rede corporativa é feito de forma totalmente livre e exposta (sem a utilização de *Secure Web Gateways/ DNS Protection,* ou outras ferramentas similares), em simultâneo com a utilização de conexões VPN à rede corporativa. Este cenário aumenta consideravelmente o risco dos ativos que estão na rede corporativa.

Na sua grande maioria estas VPN's não dispõem de mecanismos de autenticação segura, nomeadamente autenticação multi-fator (MFA) e emissão de certificados para cada utilizador e/ou equipamento, tornando-as vulneráveis. Para além disso, muitos destes acessos remotos foram criados sem levar em linha de conta as reais necessidades de acesso à informação bem como da respetiva criação de perfis.



Com a informação mais dispersa e residente nos equipamentos remotos dos utilizadores finais assumem maior prioridade as ações que assegurem a proteção da informação nestes dispositivos.



A informação sensível trocada entre os diversos dispositivos torna-se nesta fase um alvo ainda mais apetecível para ameaças persistentes avançadas.

Os mecanismos de anonimização de dados, DRM (Digital Rights Management) e de DLP (*Data Loss Prevention*) aumentam a sua preponderância com o incremento massivo da quantidade e tipologia de informação extraída das redes corporativas para os *end-points* e trocadas entre estes.

Neste cenário de trabalho remoto tornam-se também mais críticos os aspetos relacionados com a proteção física dos dispositivos, encriptação de informação e o seu backup.

A capacidade de monitorização e deteção de incidentes foi ajustada?

Em muitas organizações os processos e tecnologias de deteção não foram ajustadas a esta nova realidade aumentando as superfícies de ataque.

Neste contexto, mais do que nunca, torna-se necessário adotar tecnologias, metodologias e serviços de monitorização e deteção cada vez mais focados nos *end-points*, utilizando soluções de solução de EDR (*End-point Detection and Response*) e no controlo dos acessos, utilizando, entre outras, ferramentas de UBA (*User Behavior Analytics*) para antecipação de acessos e comportamentos anómalos.

Importa também referir que as rotinas de horários fixos se esbateram. Os colaboradores, por força das circunstâncias familiares adotaram horários flexíveis e dispares entre si. Manter uma monitorização diária, de segunda a sexta, no mesmo horário diurno fixo tornou-se ainda mais insuficiente.

Aumentar a capacidade de resiliência e resposta a incidentes

Por todos estes fatores assistimos e continuaremos a assistir a um crescente numero de incidentes críticos nas organizações.

Preparar planos de resposta a incidentes e equipas para responder rapidamente na contenção e erradicação destes incidentes tornou-se ainda mais crítico para reduzir o impacto que estes incidentes provocam nas operações.

A contenção rápida de um incidente diminui drasticamente os potenciais impactos nos ativos das organizações.

Deloitte *Cyber Risk Framework*

Cyber Strategy

Apoiamos as equipas de gestão no desenvolvimento de programas de gestão de risco cibernético alinhados com os objetivos estratégicos e o apetite de risco da organização.

Secure

O nosso foco é estabelecer controlos eficazes em torno dos ativos mais sensíveis da organização. Procuramos equilibrar a necessidade de reduzir riscos com os objetivos de produtividade, crescimento das operações e otimização de custos.

Vigilant

Integramos inteligência sobre ameaças recorrendo a variadas fontes no sentido de dotar as equipas de segurança dos meios necessários para detetar e endereçar antecipadamente as ameaças e riscos de cibersegurança.

Resilient

Conjugamos processos e tecnologias para a mitigação e reação rápida a incidentes de cibersegurança, causados por vetores de ameaça internos ou externos.

Contacts

Frederico Macias
Associate Partner
+351 966 850 347
fremacias@deloitte.pt

Luís Lobo
Senior Manager
+351 911 171 619
lulobo@deloitte.pt

Ângelo Igreja
Senior Manager
+351 911 188 876
anigreja@deloitte.pt

André Pedra
Manager
+351 919 605 620
apedra@deloitte.pt

André Correia Sousa
Manager
+351 962 753 775
andrsousa@deloitte.pt

Deloitte.