#fiqueemcasa

www.auren.pt

Cibersegurança e Tecnologia

Contexto

Do ponto de vista das TICs, o estado de emergência de resposta ao COVID-19 aportou várias consequências:

- Uso massivo de teletrabalho,
- Uso de videoconferências para realizar reuniões ,
- Aumento exponencial da contratação on-line,
- Valorização da presença nas redes sociais e do e-commerce,
- Utilização de novas tecnologias (por exemplo, *big data*) para ajudar a identificar novas procuras e a oferecer serviços mais personalizados,
- Aumento de ataques cibernéticos devido ao uso massivo de tecnologia da informação, por equipas e organizações com pouca preparação para o atual cenário.

Sem um esforço conjunto na digitalização e na proteção dos seus processos e atividades, muitas empresas não conseguirão sobreviver a esta situação, que ainda pode ser agravada por sucessivas ondas da doença.

Vetores de atuação e melhoria

As ações a serem executadas pelas organizações estão agrupadas nos seguintes vetores ou linhas de ação:

Sistemas e Aplicações	Redes e Comunicações	Processos e Procedimentos

Sistemas e Aplicações:

- Expansão ou redimensionamento dos equipamentos móveis e / ou portáteis da empresa,
- Proteção de dispositivos móveis e / ou portáteis e criação de políticas de BYOD (*bring your own device* - traga o seu próprio dispositivo),
- Adaptação das infraestruturas atuais para que os sistemas e aplicações em uso pela empresa possam operar remotamente,
- Análise da capacidade e carga dos sistemas de hardware atuais para o trabalho remoto (ou da capacidade de fornecedores: aplicações, sites e sites de e-commerce, etc.),
- Avaliação da segurança e da conformidade com os atuais mecanismos de comunicação e de recrutamento nas várias plataformas/ferramentas em uso (email, chat, mensagens, videoconferência, streaming, aplicações, *Software* as a service, etc.).

Redes e Comunicações:

- Revisão e aprimoramento, quando apropriado, da largura de banda e da capacidade das redes de comunicação,
- Contratação/renegociação com fornecedores alternativos de rede e de telefone,
- Quando necessário, contratação e instalação de soluções de conectividade nas residências dos trabalhadores-chave (router 4G, fibra ótica etc.),
- Revisão do nível de acesso das redes da empresa a recursos externos, aumentando o número de serviços executados no exterior e, em alguns casos, flexibilizando as regras de funcionamento,
- Revisão e aprimoramento dos sistemas de conexão remota (VPNs) e da sua capacidade simultânea (licenças, carga da CPU, etc.),
- Revisão das regras, da configuração e da capacidade de operação dos sistemas de monitoria e segurança (ativos ou passivos) das redes da empresa, bem como dos mecanismos de registo de eventos.

Processos e procedimentos

- Análise ou revisão, quando apropriado, dos processos críticos relacionados com o bom funcionamento das TICs *(Business Impact Analysis)*,
- Melhoria dos planos e cenários de contingência de TICs, especialmente o cenário de pandemia (com base nas lições aprendidas após este primeiro trimestre),
- Criação de políticas e procedimentos para o controle de informação em comunicações, marketing e redes sociais (internas e externas) ,
- Reforço dos procedimentos de autorização (pagamentos, registos de utilizadores, alterações etc.),
- Incorporação de soluções de assinatura eletrónica - protegendo adequadamente as palavras-chave,
- Sensibilização e formação da equipa (incluindo simulações) sobre o aumento da exposição a ataques cibernéticos (phishing, fraudes, etc.) e sobre o bom uso das ferramentas e conteúdos media (email, videoconferência, aplicativos, chats, social media, etc.)