Moção Sectorial Mais Cibersegurança

XXIV Congresso Nacional do Partido Socialista

1. Referências Multibanco Fraudulentas:

Todos os anos muitos portugueses são vítimas de burlas cada vez mais sofisticadas e credíveis que usam fragilidades do sistema de Multibanco. As burlas são realizadas de várias formas, em compras online, p.ex. no OLX, o nome da EDP, da Electricidade da Madeira, da PSP Porto e muitas outras.

As entidades multibanco usadas pelos burlões são "entidades financeiras" autorizadas pelo Banco de Portugal desde 2017 e algumas surgem muito associadas a actividades criminosas. Os burlões registam-se nestas entidades deixando vários elementos de identificação e conseguem estar activos durante muitos anos com total impunidade e lesando milhares de cidadãos, a maioria dos quais idosos e que não chegam a apresentar queixa na Justiça. Tendo em conta que os criminosos se identificam nestas plataformas que isto ocorre desde 2017 é incompreensível como é que este crime continua a ser possível e o Banco de Portugal (BdP) e a SIBS ainda não tenham agido para travarem estas burlas.

É preciso resolver as lacunas que permitem a operação destes criminosos:

a. Se as empresas que vendem referências multibanco forem associadas a um grande surto de actividade criminosa devem ter a sua licença no Banco de Portugal suspensa até que a sua segurança interna seja reforçada. Embora muitas destas entidades (como a 21800 com sede na Holanda) estejam a vender serviços a burlões desde 2017 continuam a ter licença como operador financeiro no BdP.

b. A SIBS (Multibanco) deve mostrar nas ATMs o nome da entidade que gera as referências e o beneficiário final do pagamento. Se a entidade estiver associada a burlas esse alerta deve surgir na ATM. É o caso das 21800, 21312, 11249, 11893, 10241, 10611, 12167 ou 11893.

2. A venda de cartões SIM de forma totalmente desconectada da identificação do comprador é uma fragilidade explorada por actividades criminosas:

A maioria dos países requer a identificação dos compradores de cartões SIM e 28 requerem ou vão passar a requerer em breve dados biométricos para cada compra de um destes cartões. Em todo o mundo há apenas 14 países onde qualquer pessoa pode comprar um cartão SIM sem se identificar. Portugal é um deles. O Reino Unido e a Lituânia são outros. Manifestamente esta anonimidade é um problema porque permite que burlões e falsários hajam sob cobertura do anonimato e realizem assim impunemente as suas actividades criminosas.

3. Todos os equipamentos (computadores, tablets e smartphones) entregues para uso profissional a colaboradores e representantes eleitos do Estado central e das autarquias locais tenham software de antivírus e um sistema de gestão remota (MDM):
Os telemóveis do Estado (pelo menos os iPhones) não têm sistemas de MDM (gestão de dispositivos móveis): Usando, por exemplo, o Microsoft Intune – uma solução de gestão de dispositivos móveis (MDM) que permite gerir dispositivos móveis – teria sido possível definir políticas de restrição de aplicações para impedir a instalação de determinados aplicativos, como o WhatsApp, nos dispositivos iOS geridos": sendo que, assim sendo, a esta lista se deveria somar o TikTok, o WeChat e todo o software da Kaspersky e obrigar ao apagamento remoto em caso de furto ou afastamento das funções que justificaram a entrega do equipamento.

4. Existem comunicações sensíveis e de Estado a circular e a serem tomadas em redes sociais externas e sob controlo de potencias estrangeiras (WhatsApp). A instalação destas aplicações pode e deve ser barrada centralmente e de forma centralizada por MDM.
Sugerimos que:
a. Que todos os políticos em funções electivas usem apenas telemóveis de Estado: com uma lista autorizada pré-determinada de aplicações e que excluem aplicações de encriptação ponto a ponto que dependem de estruturas ou organizações estrangeiras.
b. Que seja criminalizado o uso de software de comunicações que não tenham encriptação de mensagens ponto-a-ponto, cujos servidores ou chaves estejam fora do controlo direto do governo, União Europeia ou da autarquia local onde são exercidas as funções electivas.
c. Deve existir um sistema de comunicações nacional, seguro e de acesso reservado a políticos eleitos para instituições europeias, governo e parlamento da República e autarquias locais. Este sistema deve estar fora do alcance de empresas e potências estrangeiras e garantir o acesso aos historiadores do futuro assim como a investigações judiciais. Sugerimos que esta aplicação seja desenvolvida e mantida no contexto das instituições europeias.
d. Que seja criminalmente responsabilizado quem efetuar comunicações de dados sensíveis ou instalar software em equipamentos do Estado Português susceptível de colocar em causa a segurança do equipamento.
e. Que seja criado um arquivo de comunicação digital, com o objectivo de preservar as decisões realizadas entre governantes e políticos, de forma a um dia poderem ser consultadas pelo público e mantendo assim a capacidade de académicos e historiadores no futuro conhecerem a realidade de hoje.

5. Todos os computadores do Estado e das Autarquias Locais não devem ter os utilizadores finais como administradores locais desses equipamentos:

Segurança: Ao conceder privilégios de administrador a um utilizador, este terá acesso total ao sistema operativo e poderá fazer alterações críticas, como instalar/remover software, modificar configurações de segurança e até mesmo apagar ficheiros essenciais. Isso aumenta o risco de comprometimento do sistema por malware, vírus ou outras ameaças cibernéticas especialmente em equipamentos – como o caso – com dados sensíveis para o interesse da República.
Estabilidade do sistema: Um utilizador com privilégios de administrador pode inadvertidamente fazer alterações que afetem a estabilidade do sistema ou de outras aplicações. Isso pode levar a falhas, bloqueios e problemas de desempenho.
Erros humanos: Mesmo que um utilizador seja experiente, erros podem acontecer. Um clique errado ou uma ação equívoca quando se é administrador pode ter consequências graves, como excluir arquivos importantes ou modificar configurações críticas sem intenção.
Políticas de segurança: Em ambientes organizacionais, é comum aplicar políticas de segurança rígidas para proteger informações confidenciais. Ao limitar os privilégios dos utilizadores, o Governo e a Autarquia poderia ter reduzido o risco de perda de dados e garantir a conformidade com as regulamentações de proteção de informações em vigor.
Geralmente, restringir os privilégios de administrador para os utilizadores finais dos equipamentos é uma prática recomendada para manter a segurança, a estabilidade e a integridade do sistema operativo e dos dados armazenados. Os utilizadores devem ter apenas as permissões necessárias para realizar suas tarefas diárias, enquanto os privilégios de administrador devem ser reservados para administradores de sistemas informáticos.
Estas obrigações devem ter a força de lei.

1º SUBSCRITOR: Rui Martins
MILITANTE Nº 132179
SECÇÃO/FEDERAÇÃO: Alvalade/FAUL
SECÇÃO TEMÁTICA: Democracia Participativa/FAUL