Saúde e (Ciber)Segurança: uma questão de vida ou de morte

dinheirovivo.pt/opiniao/saude-e-ciberseguranca-uma-questao-de-vida-ou-de-morte-12786849.html

26 de abril de 2019

O setor da saúde está cada vez mais "digital" ...

O histórico do paciente passou a estar à distância de um clique, as receitas são agora eletrónicas e os equipamentos necessários para conduzir uma operação clínica estão cada vez mais interligados em rede! Apesar da resistência inicial da comunidade "hospitalar" - leia-se: pacientes, administrativos, assistentes, enfermeiros e médicos - que, agora, dificilmente aceitariam regressar a um cenário pré-digital.

A época digital do setor da saúde é uma inevitabilidade e, assim cremos, uma inevitabilidade positiva, mas, como em todas as "revoluções", implica também ter que assumir um conjunto de novos desafios.

Se é verdade que arquivos em papel, repletos de dados privados de pacientes, deixaram de estar à mercê do "amigo do alheio" - ou de, vejamos, uma mera inundação - esses mesmos dados, agora em arquivos "digitais", passam a estar à mercê de um "amigo do alheio" muito particular: o cada vez mais conhecido cibercriminoso. A este novo "amigo do alheio", deixa de ser requerida a coragem de entrar num hospital, basta-lhe penetrar na fronteira virtual do hospital e aceder aos sistemas mais valiosos ou interessantes, através de qualquer que seja o dispositivo, no conforto do seu sofá, onde quer que esse sofá se localize.

Se é verdade que receitas passadas à mão estavam sujeitas, facilmente, a adulteração para os mais distintos propósitos e que, agora, sendo eletrónicas, agilizam processos e evitam abusos, também é verdade que, daqui em diante, ficam expostas a outros cenários de

criminalidade ou acesso ilícito que podem colocar em causa a confidencialidade, integridade ou disponibilidades dos mesmos Por exemplo, com um simples ataque de DoS (Denial of Service), e não sendo as infraestruturas de segurança capazes de responder adequadamente, os sistemas e respetivos dados clínicos podem ficar inacessíveis por períodos indeterminados, bloqueando a eficiência – até ao limite da inoperabilidade - de qualquer hospital.

Se é verdade que a conetividade dos equipamentos, a comunicação entre sistemas – a interoperabilidade – ou a inteligência artificial podem revolucionar, brutalmente, a medicina e contribuir, como nunca antes, para a eficaz defesa do valor (*qualidade de)* vida dos cidadãos - em última análise é o propósito do setor da Saúde! - também é verdade que podem prejudicar, atrozmente, esse valor, não porque o profissional não esteja capacitado para a sua atividade, mas porque está, agora, dependente do acesso imediato à informação e, por inerência, à obrigação da operacionalidade e segurança dos sistemas e equipamentos que o suportam no decorrer da sua atividade. Contudo, essa mesma estrutura de sistemas, equipamentos e informação estão "disponíveis" para serem atacados como nunca antes e podem, agora, ser alvo de inúmeras ameaças que podem comprometer, violentamente, toda a atividade do setor hospitalar e dos seus pacientes, como nunca aconteceu em outra geração.

Se fizermos uma análise em retrospetiva, podemos aferir uma panóplia de casos que exemplificam a fragilidade do setor:

Em 2014, o Boston's Children Hospital sofreu um ataque de DoS, perpetrado pelo conhecido grupo de hacktivistas Anonymous, em reação à mediática batalha pela custódia de Justina Pelletier entre o referido hospital e a sua família. O responsável pelo ataque foi apenas condenado no ano passado.

Entre maio de 2015 e julho de 2018, o sistema nacional de saúde de Singapura sofreu uma das mais sérias perdas de dados pessoais, em resultado de um ciberataque. Entre os 1,5 milhões de dados obtidos, encontrava-se a informação privada do Primeiro Ministro Lee Hsien Loog.

Já em 2016, dois casos de ransomware ficaram na história do setor da saúde dos Estados Unidos, um pela positiva, outro pela negativa. Enquanto o Hollywood Presbyterian Medical Center, vítima do chamado Locky, viu o seu acesso à rede impedido até ao pagamento de um resgate de 17 mil dólares, tendo só, posteriormente, comunicado o sucedido às autoridades, o segundo, o Ottawa Hospital, viu os seus dispositivos encriptados, depois de um ataque de phishing aos seus funcionários, que abriram, inadvertidamente, um email malicioso. Contudo, porque o Hospital tinha cópias de segurança de toda a sua informação, limitaram-se a limpar e repor a informação nos discos, e não pagaram o resgate.

No mesmo ano, o Hospital Garcia da Horta foi alvo de um ataque informático que incidiu sob o sistema onde estão guardadas as imagens obtidas em exames médicos, como radiografias ou TAC.

Fazendo um parêntesis temporal, há que ressalvar que este caso é particularmente alarmante, contando que, no início deste mês, quatro investigadores da Ben-Gurim University CyberSecurity Research Center, em Israel, criaram um malware capaz de apagar o rasto/criar um falso rasto de nódulos cancerígenas em TACs ou ressonâncias magnéticas e enganar qualquer especialista, num teste particularmente bem-sucedido. O simulacro de ataque – que poderia funcionar com tumores cerebrais, doenças do coração, coágulos no sangue, lesões da coluna, fraturas ósseas, lesões dos ligamentos ou artrite – serviu para demonstrar a vulnerabilidade dos hospitais, mais concretamente dos seus equipamentos e rede, e da importância de conceitos tão fundamentais para a cibersegurança como são a integridade, autenticidade ou encriptação da informação que armazenam e utilizam diariamente no decorrer da sua atividade.

Retomando as evidências, em 2017, ao mesmo tempo que um dos mais violentos ataques, o WannaCry, afetava empresas e instituições por todo o mundo, nomeadamente, hospitais no Reino Unido e Ásia, os Serviços Partilhados do Ministério da Saúde (SPMS) pediram às instituições de cuidados de saúde portuguesas que se desconectassem da internet, como medida de prevenção. Ou seja, e em termos práticos, ao acionar uma medida desta dimensão – leia-se desligar-se do mundo cibernauta – estamos obviamente a assumir a nossa incapacidade – refira-se também, por inerência, a nossa vulnerabilidade - para responder a um ataque desta escala e, então, assumir que temos que decidir por "parar a saúde", literalmente, para não sermos alvo de um ciberataque. Esta reação apenas demonstra a imaturidade do sector hospitalar – entre outros – no que respeita ao tema da cibersegurança. No mesmo ano, meses depois, o NotPetya, outro célebre ciberataque de grande escala, também afetou, entre várias organizações, sistemas de cuidados de saúde americanos.

Mais recentemente, no cenário português, dois casos distintos estiveram na ordem do dia. Por um lado, o Hospital do Barreiro, multado em 400 mil euros por má política de acesso e acesso indevido às bases de dados de pacientes que, no âmbito dos direitos dos titulares dos dados, agora com a agravante do RGPD, colocava em causa inclusive a privacidade dos seus dados pessoais. Por outro, o sistema dos hospitais CUF do grupo José de Mello Saúde, sofreu um ataque de ransomware, exigindo o pagamento de 10 milhões de euros, o que paralisou o serviço e obrigou ao cancelamento de várias consultas e respetivos tratamentos. São ainda desconhecidos a verdadeira amplitude e impacto deste ataque no que respeita ao acesso e a violação dos dados envolvidos no referido ataque.

Em suma, importa frisar o valor que a cibersegurança e a proteção de dados, em especial, dos dados de maior criticidade ou sensibilidade – designados no RGPD como classificação "especial" de dados – são muitas vezes postos em causa pela ausência de uma verdadeira cultura do tema da cibersegurança entre os gestores de algumas das mais relevantes instituições ou organizações nacionais. A comunidade de colaboradores de uma entidade do sector da saúde tem um espetro académico muito lato e nem sempre devidamente instituído. Consideram-se assim, fundamentais na sociedade moderna, digital e democrática o desenvolvimento dessas competências, como pressupostos de atuação em qualquer setor, quanto mais no setor da saúde. É precisamente na camada de gestão dessas organizações que deve começar a implantação e atualização da cultura da

segurança de informação juntos dos seus colaboradores para que o mundo virtual seja também cada vez mais seguro, quer se trate dos seus utilizadores – pacientes até médicos – quer envolva a própria segurança da infraestrutura que suporta a atividade do hospital.

Não basta ser-se hipertecnológico e representar todas as modas e tendências, aderindo ao último grito de "tablets que tiram cafés, cafeteiras com inteligência artificial ou drones dobráveis em 10G". Se não tivermos consciência do potencial – em todos os sentidos – do mundo virtual em que vivemos, e se não formos capazes de culturalmente nos adaptarmos às ameaças também virtuais – mas de carater real – nunca seremos capazes de nos protegermos devidamente e, então, a evolução tecnologia poderá vir a ser um dos piores truques de magia da era digital.