Naar een informatief en digitaal veilig 2021

En zo eindigde 2020… en begint 2021: met een cyberincident van ongekende proporties. De SolarWinds-hack raakt de Verenigde Staten diep in het hart. Duizenden ICT-systemen van overheid en bedrijfsleven zijn maandenlang toegankelijk geweest voor – naar verluidt – Russische daders. De consequenties liggen in de toekomst verborgen. Ook voor Nederland, zoals bleek uit hacks rondom Pulse Secure (2019) en Citrix (2020), waarbij het beveiligd inloggen vanaf de thuiswerkplek in het geding was. De potentiële risico's zijn inmiddels enkel groter geworden met de toegenomen online afhankelijkheid vanwege Covid-19.

In oktober wees generaal Jan Swillens, directeur MIVD, in *De Telegraaf* nadrukkelijk op deze gevaren. Onder de kop 'Smartphones van tafel tijdens vergadering' waarschuwde hij voor de bespreking van bedrijfsgeheimen met smartphone of tablet in de buurt. David Omand, gerenommeerd Brits veiligheidsdeskundige, liet in december eveneens een waarschuwing horen. In een interview benadrukte hij de gecompliceerde multipolaire veiligheidssituatie (met statelijke en non-statelijke, externe en interne dreigingen), de steeds grotere rol van (des)informatie en daaruit voortvloeiende veiligheidsconsequenties, en de revolutionaire ontwikkelingen op datagebied, die informatieveiligheid (cyber security) tot absolute topprioriteit maken.

Is het belang van informatiezekerheid en de vereiste digitale beveiliging voldoende tot ons doorgedrongen? De Nederlandse overheid maakt geen solide indruk op dit vlak. Enkele voorbeelden: Buitenlandse Zaken kreeg – bij herhaling – een rode kaart van de Algemene Rekenkamer vanwege de deplorabele staat van informatiebeveiliging. Om die reden dreigden de NAVO en EU al in 2019 geen digitale documenten meer naar Den Haag te sturen. PulseSecure en Citrix maakten pijnlijk duidelijk dat 'cyberwaakhond' NCSC niet als een daadwerkelijk Nationaal Cyber Security Centre fungeert. En door onoplettendheid binnen Defensie verkreeg een journalist afgelopen november toegang tot een vertrouwelijke onlinevergadering van Europese defensieministers. Wie op internet zoekt, vindt in milliseconden lijsten van grote cyberhacks. Bedrijven en overheden liggen continu onder vuur. Dit raakt Defensie en, niet te vergeten, de defensie-industrie. Om toekomstbestendig te zijn kan Defensie niet zonder veilige en 'grensverleggende' informatietechnologie (GrIT). Helaas heeft Defensie wat betreft ICT-ontwikkeling bepaald geen smetteloos blazoen. Zo verbrandde Project Speer honderden miljoenen euro's en kende GrIT een afgedwongen 'pauze' van zestien maanden vanwege ernstige twijfel over de slagingskans van dit peperdure IT-infrastructuurproject.

Op de oproep van directeur-MIVD werd positief gereageerd, al viel soms een ondertoon van meewarigheid te bespeuren. Noodzaak en gemak van smartphone en tablet zijn van deze tijd en wie wil er terug naar de vorige eeuw? Hoe opportuun is een dergelijke oproep wanneer iedereen geacht wordt thuis te werken? Maar in een gedigitaliseerde wereld waar cyberincidenten aan de orde van de dag zijn, is passiviteit rond informatiezekerheid geen optie. Ongeautoriseerde toegang kan slechts één stap verwijderd zijn van sabotage en op dergelijke cyberincidenten zit niemand te wachten.

De *Militaire Spectator* wenst iedereen een informatief en digitaal veilig 2021. ■