Reactie EPZ op uitzending malware Zembla

7 oktober 2021 - 17:27

De redactie van Zembla heeft voor haar actualiteitenprogramma een algemene screening uitgevoerd op de emailbeveiliging van EPZ en trekt de conclusie dat die onvoldoende zou zijn. Echter, Zembla kan op afstand niet alle bij EPZ aanwezige email-securitymaatregelen zien. Die zijn robuuster dan uit de Zembla-screening blijkt. Zonder al te veel in detail te gaan: EPZ beschikt over een effectief, door de overheid goedgekeurd beveiligingspakket. Het berichtenverkeer van en naar EPZ is niet direct aan internet gekoppeld. Bovendien vindt in deze losgekoppelde omgeving controle plaats op de betrouwbaarheid van mailberichten.

Net als iedere andere Nederlander of Nederlandse organisatie staat ook EPZ bloot aan de door Zembla geschetste criminele methodes. EPZ is geen uitzondering. Juist omdat EPZ goed weerstand kan bieden aan cybercriminaliteit en dit permanent monitort, kan EPZ stellen dat geen enkele poging succesvol was. Er waren dus wel pogingen, maar die hebben niet tot incidenten geleid. Er is overigens een meldingsplicht voor incidenten met (middel) grote impact. Er was geen schade en er hoefde dus ook geen melding te worden gedaan bij de toezichthouders.

Uiteraard is EPZ altijd alert op verbeteringen. Dit geldt voor alles wat onze veiligheid en beveiliging betreft. Alle NCSC-veiligheidsmeldingen komen bij EPZ terecht bij de IT-security betrokken personen. Vervolgens wordt beoordeeld of ze van toepassing zijn op de

ICT-inrichting van EPZ: het nut en de noodzaak. Indien dat het geval is dan wordt de aanbeveling aansluitend doorgevoerd. De snelheid van doorvoeren is afhankelijk van de combinatie “kans (dat een kwetsbaarheid benut wordt) x effect (dat hierdoor kan worden veroorzaakt)”.

De security-aanscherping (DMARC) waarop de redactie van Zembla focust, geldt uitsluitend voor vanuit EPZ verzonden emailberichten. De beveiliging van de uitgaande mailberichten werd juist ten tijde van het contact met Zembla bij EPZ onderzocht. Een deel van de adviezen was toen al overgenomen. Een ander deel van de adviezen voor uitgaande email werd op dat moment nog onderzocht. Daarvan stond de meerwaarde voor de beveiliging van uitgaande mail nog niet vast. Later in september volgde de afronding van de implementatie van de striktere DMARC-policy voor uitgaand emailverkeer.

Kerncentrale niet via internet te benaderen

Het reactorbeveiligingssysteem van de kerncentrale is analoog. Dit kan dus per definitie niet gehackt worden. In de kerncentrale is geen enkel vitaal bedieningssysteem aangesloten op het internet. De procesinstallaties zijn van buitenaf dus niet benaderbaar. Het aansturen van het nucleaire proces en de bediening van de reactor gebeurt met analoge techniek die ongevoelig is voor digitale verstoringen. Verstoring van ICT-systemen rond de kerncentrale heeft daarom geen invloed op de beschikbaarheid van de bedieningsinstrumenten. Deze staan immers helemaal los van ICT-aansturing. De overige in onze kerncentrale aanwezige ICT- systemen zijn slechts ondersteunend en worden bovendien streng beveiligd.