Bijlage C – Relevante bedreigingen

De volgende bedreigingen zijn in de analyse meegenomen:

1. Een gerichte ransomware aanval met geavanceerde software.
2. Ongerichte malware.

   Malware / ransomware is een algemeen hoofdpijn-onderwerp voor beveiligers. De Informatiebeveiligingsdienst (IBD) heeft voor scenario 1 een gerichte waarschuwing vertrouwelijk doen uitgaan over de situatie in Nederland waar (1) gerichte activiteit is, (2) concrete voorbeelden zijn, (3) soorten zwakheden gebruikt worden die ook bij Haarlem aanwezig zijn.

3. Menselijke vergissingen, nalatigheid en het niet hebben van de vaardigheid of de middelen om veilig te werken. Hierbij horen ook het verlies van een telefoon, tablet of USB-stick.

   Iedere week staan er voorbeelden in de krant.

4. Gerichte actie door een deskundige externe partij via Internet. Hieronder valt ook de hacker die wil ingrijpen in de besturing van bijvoorbeeld bruggen en verkeersregelinstallaties.

   Uit loggings blijkt dat de omgeving van Haarlem vanaf Internet continu wordt afgetast. Driemaal is een account door een onbekende partij overgenomen, bij onderzoek is duidelijk geworden dat nog 4 wachtwoorden extern bekend waren geraakt.

5. Gerichte actie door een deskundige externe partij die zich in Haarlem bevindt, en die lokale aanwezigheid (bv. Insluipen, toegang tot kabels, fysiek beschadigen of ontvreemden van apparaten, openbreken van kasten) toevoegt aan de mogelijkheden van toegang via Internet.

   Dit is het Hoffmann scenario dat de RKC heeft gevolgd.

6. Een security incident dat te maken heeft met een leverancier.

   We kunnen ook verantwoordelijk zijn als het niet aan ons ligt. Hiervan staat regelmatig een voorbeeld in de krant.

7. Een fysiek incident waardoor een heel gebouw niet kan worden gebruikt.

   Er wordt uitgegaan van eens per 30 jaar per gebouw.
   Het gaat dan om zaken als lekkage (hemelwater, leidingbreuk) waardoor de stroom afgesloten moet worden, om bluswerkzaamheden of andere redenen waardoor een brandweercommandant een gebouw spanningsloos maakt, of uitval van nutsvoorzieningen (voorbeelden als regio Amsterdam voor stroom, regio Groningen voor water)

Op de volgende pagina staat ter illustratie een lijst met actuele voorbeelden

Ongerichte malware:

- https://www.nctv.nl/actueel/nieuws/2019/csbn-2019-ontwrichting-maatschappij-ligt-op-de-loer.aspx
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- https://en.wikipedia.org/wiki/2018_Atlanta_cyberattack
- https://statetechmagazine.com/article/2019/04/more-year-after-atlanta-ransomware-attacks-cities-remain-vulnerable
- https://tweakers.net/nieuws/154248/amerikaanse-stad-betaalt-534000-euro-losgeld-na-ransomwareaanval.html

Menselijke vergissingen e.d:

- https://assercourant.nl/artikel/1013055/datalek-gemeente-assen-honderden-persoonsgegevens-in-verkeerde-handen.html
- https://destadamersfoort.nl/lokaal/gemeente-amersfoort-opnieuw-opgeschrikt-door-datalek-456914
- https://opgelicht.avrotros.nl/nieuws/artikel/24-datalekken-bij-gemeente-amsterdam/
- https://www.tubantia.nl/hengelo/hengelo-extra-controle-automatische-mails-na-datalek
- https://www.leidschdagblad.nl/cnt/dmf20190620_68097278/alphen-aan-den-rijn-neemt-werkprocessen-onder-de-loep-na-groot-datalek
- https://www.security.nl/posting/581385/Heathrow+krijgt+boete+voor+verlies+onversleutelde+usb-stick

Gerichte actie door een goed voorbereide externe partij via Internet:

- https://en.wikipedia.org/wiki/2018_Atlanta_cyberattack
- https://statetechmagazine.com/article/2019/04/more-year-after-atlanta-ransomware-attacks-cities-remain-vulnerable
- https://tweakers.net/nieuws/154248/amerikaanse-stad-betaalt-534000-euro-losgeld-na-ransomwareaanval.html
- https://www.omroepzeeland.nl/nieuws/102548/Hacken-sluizen-en-gemalen-nog-steeds-mogelijk
- https://www.securitymanagement.nl/waterwerken-nog-altijd-te-hacken/

Leveranciers:

- https://tweakers.net/nieuws/118607/gestolen-laptop-veroorzaakt-mogelijk-datalek-bij-verschillende-gemeenten.html
- https://www.agconnect.nl/artikel/datalek-anwb-komt-door-it-leverancier
- https://tweakers.net/nieuws/140337/ticketmaster-uk-waarschuwt-deel-van-gebruikers-voor-datalek-via-leverancier.html
- https://www.security.nl/posting/613131/Datalek+Neckermann+na+diefstal+van+computers+en+laptops
- https://www.securityweek.com/wetransfer-security-incident-file-transfer-emails-sent-wrong-people