Ransomware

INFORMATIE BEVEILIGINGS DIENST

Ransomware (gijzelsoftware) is malware die data versleutelt met als doel deze later in ruil voor losgeld te ontsleutelen. In de ergste gevallen is de systeemtoegang geblokkeerd en dreigen de criminelen om gestolen data online te publiceren als geen losgeld wordt betaald.[1]
Hoe een ransomware aanval er uit ziet en welke maatregelen ingezet kunnen worden ziet u in bijgaand schema.[2]

Ransomware aanval

Initiële toegang

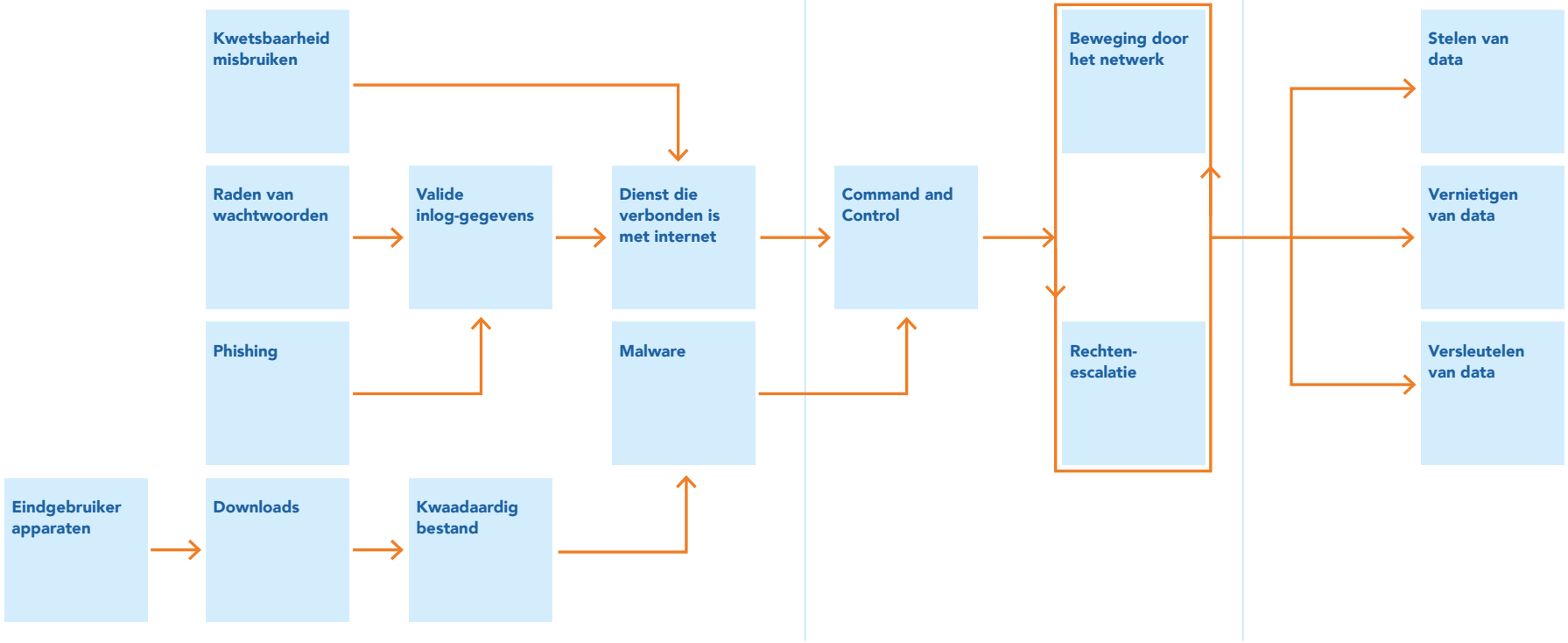
Aanvallers zoeken een manier om toegang te krijgen tot het netwerk van de gemeente.

Voorbereiden en verhogen van rechten

Aanvallers proberen toegang te krijgen tot alles binnen het gemeentelijk netwerk.

Impact voor de gemeente

Aanvallers stelen, vernietigen en/of versleutelen data en eisen daarna losgeld.



Figuur 1: Een aanvaller zoekt een manier om in het netwerk te komen en kan daarvoor verschillende manieren gebruiken. Eénmaal binnen in het netwerk zal een aanvaller zichzelf zo hoog mogelijke rechten willen toekennen. Daarna zal een aanvaller data kunnen stelen, vernietigen en/of versleutelen.

1. https://www.ncsc.nl/onderwerpen/ransomware
2. Hiervoor is ter inspiratie gekeken naar: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Maatregelen tegen ransomware aanval

Initiële toegang

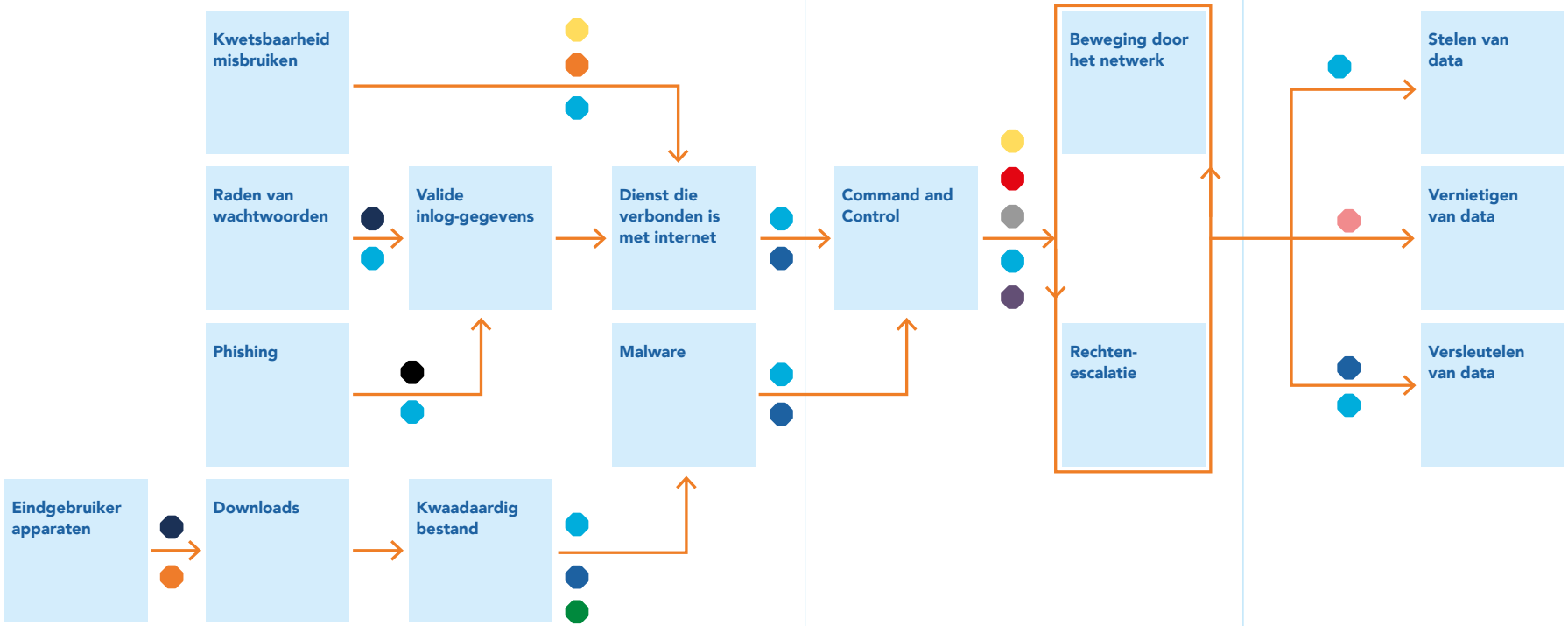
Aanvallers zoeken een manier om toegang te krijgen tot het netwerk van de gemeente.

Voorbereiden en verhogen van rechten

Aanvallers proberen toegang te krijgen tot alles binnen het gemeentelijk netwerk.

Impact voor de gemeente

Aanvallers stelen, vernietigen en/of versleutelen data en eisen daarna losgeld.



Figuur 2: Maatregelen om het een aanvaller zo moeilijk mogelijk te maken zijn per fase waar ze van toepassing opgesomd. Omdat het lastig is om alle maatregelen direct volledig te implementeren is een voorzet voor de prioritering op de volgende pagina verder beschreven.

VDW #1
- Hardening
- Patching
- MFA
- Netwerksegmentatie
- Least Privilige principe
- Applicatie Whitelisting
- Uitschakelen Macro's

VDW #2
- Logging en alerting

VDW #3
- Bewustwording

VDW #4
- Back-ups

De IBD heeft verschillende producten die verder ingaan op de verschillende maatregelen. Zie hiervoor de verschillende Verhoging Digitale Weerbaarheidsmodulen[3] en een overzicht van verschillende bewustwording campagnes[4] op de website van de Informatiebeveiligingsdienst.

Overzicht van de belangrijkste maatregelen tegen ransomware met een focus op de belangrijkste aandachtsgebieden:

Maatregel	**Voorzet van prioritering** (Let op: dit is niet alles maar geeft een prioriteit waar dit het effectiefst kan zijn)
MFA	Minimaal MFA aanzetten op webmail, internet facing management interfaces, office 365, RDP *(liever uitzetten; zie maatregel "hardening"), beheeraccounts en VPN. Zeer belangrijke maatregel die de kans en impact van incidenten zoals Lochem en Hof van Twente had kunnen verlagen.*
Hardening	Diensten die verbonden zijn met het internet minimaal RDP uitzetten (er zijn betere oplossingen voor remote beheer). Eindgebruiker apparaten dienen voorzien te zijn van virusscanners…. *Belangrijke maatregel die de kans en impact van incidenten zoals Lochem en Hof van Twente had kunnen verlagen.*
Bewustwording	Bewustwordingsprogramma met een focus op het herkennen van verdachte situaties (bijv. phishing) en hoe medewerkers dienen te acteren bij een potentieel incident. Ook het belang van bewustwording van goede unieke wachtwoorden in combinatie met MFA is belangrijk.
Patch management	Goed patch management proces met minimaal een focus op het snel oplossen van High/High kwetsbaarheden na ontvangen melding van de IBD.
Netwerk segmentatie	Een overzicht krijgen van de verschillende data stromen binnen het netwerk en daarmee segmentatie toepassen van o.a. werkstations, servers, management interfaces en extern gerichte netwerken.
Logging en monitoring	Minimaal alerting aanzetten op verschillende logbronnen. *(bijv. standaard alerts op virusscanner, firewall en IDS) Dit inzichtelijk maken met dashboards voor structurele borging. Daarnaast dienen het toekennen van administrator rechten gemonitord te worden; aanvallers zullen hun rechten willen verhogen.*
Back-ups	Breng in kaart hoe dit geregeld is binnen uw gemeente, kijk naar kritische systemen binnen de processen van uw gemeente en breng daar de prioriteit voor aan. Richt een proces in om automatisch bestanden te restoren en te vergelijken, als die niet vergeleken kunnen worden dient er een alarmbel af te gaan. Kwaadwillende vallen gericht de back-ups aan met als doel een restore onmogelijk te maken na versleuteling.
Least privilige	Belangrijk dat (global/technische) admin accounts zijn losgekoppeld van het gewone gebruikersaccount en dat eindgebruikers geen local admin zijn op hun door de gemeente beheerde apparaten.

3. https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/
4. https://www.informatiebeveiligingsdienst.nl/project/bewustwording/