(Pers-)berichten

Fundamenteel ingrijpen is nodig voor Nederlandse digitale veiligheid

De Nederlandse aanpak van digitale veiligheid moet snel en fundamenteel veranderen om te voorkomen dat de maatschappij ontwricht raakt door cyberaanvallen. Dat concludeert de Onderzoeksraad voor Veiligheid in het vandaag gepubliceerde rapport 'Kwetsbaar door software'. De Onderzoekraad onderzocht beveiligingslekken die ontstonden bij duizenden organisaties door kwetsbaarheden in software van Citrix. Jeroen Dijsselbloem, voorzitter van de Onderzoeksraad voor Veiligheid: "Uit dit voorval blijkt dat Nederlandse overheidsorganisaties en bedrijven zeer kwetsbaar zijn voor cyberaanvallen en dat er geen nationale structuur is waarbinnen alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd."

Aanvallen via Citrix

Op 17 december 2019 maakte Citrix een kwetsbaarheid in zijn software bekend en nam het bedrijf tijdelijke maatregelen om de risico's te beperken. Nog voordat de vele duizenden Citrix-gebruikende organisaties doordrongen waren van de acute risico's en de tijdelijke maatregelen hadden geïnstalleerd, waren aanvallers binnengedrongen in systemen. Het Nationaal Cyber Security Centrum (NCSC) waarschuwde direct het deel van de Nederlandse gebruikers waarvoor zij zich verantwoordelijk achtte: overheidsdiensten en vitale organisaties. Andere organisaties werden door het NCSC niet gewaarschuwd. Aanvallers konden nog steeds op grote schaal digitale systemen binnendringen. Tot op de dag van vandaag hebben zij daarmee illegale toegang tot systemen en data in bedrijven en organisaties die zij op elk moment kunnen activeren met disruptieve effecten op bedrijfsprocessen, dienstverlening, privacy en veiligheid.

Verantwoordelijkheid fabrikanten

Veilige software is allereerst de verantwoordelijkheid van de fabrikant. De Onderzoeksraad stelt dat fabrikanten meer zouden moeten investeren om de veiligheid van software voortdurend te verbeteren. Fabrikanten overstelpen softwaregebruikers nu met patches en updates om gebreken in hun software te verhelpen zonder met structurele oplossingen te komen. Er zijn geen instrumenten die afnemers van software onafhankelijk inzicht bieden in de veiligheid van de software. Ook schiet de eigen kennis en positie van afnemers vaak tekort om zelf eisen te stellen aan fabrikanten en veiligere software af te dwingen, of zien zij daar het belang niet van in.

Beperkte overheidsaanpak

Veel organisaties die software gebruiken en potentieel slachtoffer zijn van cyberaanvallen worden nu niet gewaarschuwd. Het NCSC ziet voor zichzelf wettelijk geen mandaat om organisaties buiten de overheidsdiensten en vitale organisaties te waarschuwen. Het is volgens de Onderzoeksraad van groot belang dat er vanuit de overheid een centrale aanpak komt om dreigingen te signaleren en alle potentiële slachtoffers van cyberaanvallen zo snel en direct mogelijk te waarschuwen, met voldoende mandaat en wettelijke waarborgen.

Aanbevelingen van de Onderzoeksraad

De samenleving wordt namelijk steeds afhankelijker van digitale systemen. Fabrikanten, overheden en organisaties zullen samen tot een effectieve aanpak moeten komen om Nederland weerbaarder te maken tegen cybercriminaliteit. Dit vraagt van fabrikanten dat zij de veiligheid van hun software voortdurend en fundamenteel verbeteren. De Onderzoeksraad doet de aanbeveling om op Europees niveau kwaliteitseisen aan software te stellen om softwarefabrikanten te dwingen verantwoordelijkheid te nemen voor de veiligheid van hun product. De Onderzoeksraad adviseert overheden en het bedrijfsleven hun krachten te bundelen. Door samen te werken kunnen ze hun positie richting softwarefabrikanten versterken en hun schaarse expertise beter benutten.

Binnen de overheid kan de bewaking van de digitale veiligheid worden geregeld zoals de bewaking van het voeren van zorgvuldig begrotingsbeleid is vastgelegd in de Comptabiliteitswet. Dat vergt dat er één bewindspersoon en een centrale dienst komt die hierop toeziet, zo nodig kan ingrijpen en verantwoording aflegt. Ook beveelt de Raad aan dat grotere bedrijven en organisaties wettelijk worden verplicht om verantwoording af te leggen over de wijze waarop zij hun digitale veiligheid beheersen.

Het rapport en de aanbevelingen staan op de onderzoekspagina: https://www.onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software-lessen-naar-aanleiding-van