SR STRAFRECHT UPDATES

ANNOTATIE

Computervredebreuk, artikel 138ab Sr.

mr. J.H.J. Verbaan

Annotatie bij Hoge Raad, 09-04-2019, ECLI:NL:HR:2019:560 (SR-2019-0096)

De verdediging klaagt namens verdachte, ten aanzien van wie computervredebreuk als bedoeld in artikel 138ab Sr is bewezen verklaard, onder meer dat de bewezenverklaring van het ten laste gelegde voor zover inhoudende dat de verdachte is 'binnengedrongen' in een deel van een geautomatiseerd werk niet uit de gebezigde bewijsmiddelen kan worden afgeleid. Het hof heeft de bewezenverklaring doen berusten op een proces-verbaal van de politie-eenheid Rotterdam-Rijnmond, inhoudende de verklaring van aangever, namens het bedrijf:

'Mijn functie binnen het bedrijf is Information Security Officer en als zodanig ben ik belast met de netwerkbeveiliging van het bedrijf. Binnen de netwerk topologie van het bedrijf is een server aanwezig genaamd bedrijf-DMZ-01. Op deze server draait een web-applicatie. Deze webapplicatie is vanaf het internet te bereiken op het adres [website] en staat binnen het bedrijfdomein in een DMZ (Demilitarized Zone).

Genoemde web-applicatie wordt gemonitord door een bedrijf genaamd Secode. Dit bedrijf monitort de website door middel van een intrusion protection system. Het bedrijf Secode heeft op 12 december 2011 een mail verstuurd dat er een aanval op de website werd uitgevoerd. Tevens werd door Secode een log bestand aangeleverd die de gegevens van de uitgevoerde aanval bevatte. In dit log bestand van Secode was te zien dat er gebruik is gemaakt van de web vulnerability scanner genaamd Acunetix. Ik zag dat er door middel van de tool Acunetix naar verschillende kwetsbaarheden in de website waren gezocht waarvan er een aantal werden geblokkeerd. Verder zag ik dat er sommige aanvallen voorzien waren van de actie Permit. In verband met deze toestemming is het niet ondenkbaar dat er een geslaagde aanval heeft plaatsgevonden. De aanval zou zijn uitgevoerd vanaf een statische IP-adres. De tijdsduur van

deze aanval uitgevoerd vanaf dit IP-adres op 12-12-2011 was gelegen tussen de tijdstippen 13:10 CET tot 13:14 CET en 16:35 CET tot 16:41 CET. CET staat voor Central European Time.

Op 14 december 2011 werd ik telefonisch door Secode op de hoogte gesteld van een langdurige aanval op de website. Door Secode werd een log bestand aangeleverd waarop te zien is dat er middels cross site scripting en directory traversal aanvallen op de website zijn uitgevoerd. Verder is er op de log te zien dat er diverse pogingen met betrekking tot Cross Site Scripting worden geblokkeerd. Ook is te zien dat door middel van Directory Traversal werd getracht in de root van de server te komen. In hoeverre deze aanval geslaagd is, is tot op heden bij ons niet bekend. Echter aangezien er diverse aanvallen zijn die zijn voorzien van de actie Permit is het niet ondenkbaar dat er een geslaagde aanval heeft plaatsgevonden.

Deze aanval is uitgevoerd vanaf een dynamische IP-adres. De tijdsduur van de aanval vanaf dit IP-adres uitgevoerd op 12-12-2011 was gelegen tussen de tijdstippen 23:01 CET en 23:03 CET.'

Daarnaast heeft het hof een verklaring van de verdachte voor het bewijs gebezigd. De verdachte heeft ter terechtzitting in hoger beroep, zakelijk weergegeven, verklaard dat Acunetix aangeeft of en zo ja, welke zwakheden er zijn geconstateerd. Daarna kun je met Acunetix handelingen verrichten om daadwerkelijk binnen te dringen.

De Hoge Raad overweegt dat het hof geen nadere bewijsoverwegingen heeft opgenomen, De Hoge Raad overweegt dat de tenlastelegging en bewezenverklaring toegesneden zijn op artikel 138ab lid 1 Sr. Daarom moet de in de tenlastelegging en bewezenverklaring voorkomende term 'binnengedrongen' geacht worden aldaar te zijn gebezigd in dezelfde betekenis als toekomt aan de term 'binnendringt' in dat artikel. De Hoge Raad haalt de bepaling aan, zoals dat luidde ten tijde van het bewezen verklaarde en overweegt dat de delictsbestanddelen gelijkluidend zijn aan die van de huidige, op 1 juli 2015 in werking getreden, bepaling. De Hoge Raad oordeelt dat de bestreden uitspraak niet naar de eis der wet met redenen is omkleed aangezien de bewezenverklaring, voor zover inhoudende dat de verdachte is 'binnengedrongen' in een geautomatiseerd werk of in een deel daarvan, niet zonder meer kan worden afgeleid uit de gebezigde bewijsmiddelen. De enkele omstandigheid dat de verdachte blijkens bewijsmiddel 3 op 12 september 2012 met behulp van een scanprogramma de website van de aangever op kwetsbaarheden heeft onderzocht, waarvan een aantal werd geblokkeerd en dat als gevolg daarvan 'niet ondenkbaar is dat er een geslaagde aanval heeft plaatsgevonden' volstaat daartoe niet. De Hoge Raad oordeelt dat de vermelding in een bewijsmiddel van aanvallen door middel van '*cross site scripting*' en '*directory traversal*' waarvan de werking niet nader is toegelicht dat niet anders maakt, in aanmerking genomen dat aldus zonder nadere motivering die ontbreekt in het midden blijft of de verdachte toegang

heeft verworven door een technische ingreep of dat het bij een poging daartoe is gebleven.