

Delen van de broncode van Microsofts besturingssysteem Windows 2000 circuleren sinds medio vorige week op internet. Ook componenten als de webbrowser Internet Explorer 5.0 en de Windows Media Player zijn uitgelekt. Het gaat om een beperkt deel – circa 8,5 miljoen regels – van de totale sourcecode. Volgens veel publicaties is ook broncode van Windows NT 4 in het geding, maar andere bronnen bestrijden dit. Microsoft neemt de zaak hoog op omdat zijn 'intellectuele eigendommen' op straat liggen. De federale opsporingsdienst FBI is een onderzoek begonnen. Er zijn aanwijzingen dat Mainsoft, een bedrijf dat onder de verplichting van geheimhouding ('non disclosure') inzage had in de broncode, de bron is van de nu uitgelekte onderdelen.

Anderzijds hoeven gebruikers zich geen zorgen te maken, stelt een woordvoerder van Microsoft Nederland: "Het lekken van delen van de broncode heeft op het ogenblik helemaal geen impact op de gebruikers. Het gaat om oude code, grotendeels van Internet Explorer 5." Inmiddels is wel een eerste 'exploit' gemeld die gebaseerd zou zijn op de uitgelekte code, maar de Microsoft-zegsman bagatelliseert dat:

Uitlekken Windows-code voor beveiliging een zegen op termijn

De meningen over de gevolgen van het uitlekken van Windows-broncode zijn sterk verdeeld. Sommige experts voorspellen een sterke toename van het aantal virussen en 'hacks'. Anderen menen dat de meeste lekken al waren gedicht.

GEERT KELFKENS

"Het betreft een lek dat al op 30 augustus 2002 via Service Pack 1 van Internet Explorer 6 is verholpen. Iedereen die deze update heeft geïnstalleerd, is helemaal veilig."

Verdeeld

Deskundigen zijn verdeeld over de vraag of het in omloop zijn van Windows-broncode ernstige consequenties heeft voor de beveiliging. Security-'goeroe' Bruce Scheier, oprichter van de firma Counterpane: "Ik ben er niet van overtuigd dat dit zo ernstig is. Hackers kunnen natuurlijk de broncode uitkammen op kwetsbaarheden. Maar tot dusver hadden ze geen moeite om die

ook zonder broncode te vinden." Een groepje Nederlandse programmeurs en IT-beveiligers heeft de broncode geanalyseerd en de resultaten op de website Securitydatabase.net gepubliceerd. Daaruit valt op te maken dat de code kwaadwillenden wel degelijk nieuwe aanknopingspunten biedt voor aanvallen op Windows-systemen. "Wij hebben ongeveer 46 duizend basale fouten gevonden", aldus een lid van deze beveiligingsgroep. "Die houden allemaal verband met zogenaamde buffer overflows. Niet alle fouten zijn uit te buiten. Je moet een exploit-code kunnen ingeven, bijvoorbeeld als ergens om een

wachtwoord of andere invoer wordt gevraagd. Maar van die 46 duizend kan misschien 1 procent wel misbruikt worden."

De woordvoerder van Securitydatabase.net meldt overigens dat de broncode inmiddels een tweede exploit heeft opgeleverd. Hij zegt verder te verwachten dat de komende tijd veel hackers die 'een reputatie willen opbouwen' fouten in Windows zullen publiceren op basis van de uitgelekte broncode.

Sneller

Rop Gonggrijp van het Amsterdamse beveiligingsbedrijf NAH6 ziet geen reden tot grote zorg. "Op

lange termijn is het beschikbaar zijn van broncode juist goed voor de beveiliging. Alle fouten zijn ook wel met omslachtiger methoden te vinden, maar bijvoorbeeld buffer overflows kun je er sneller uithalen als je de broncode hebt. Microsoft wordt nu bovendien gedwongen die lekken sneller te dichten."

Ook een andere IT-beveiliging, directeur Hans van de Looy van het Eindhovense bedrijf Madison Gurkha, verwacht – al heeft hij de uitgelekte broncode niet gezien – geen grote problemen. "Er is maar een klein gedeelte van de broncode vrijgekomen. Bovendien gaat het om Service Packs, wat in feite al verbeteringen van eerder geconstateerde fouten zijn. Ik denk dat het extra risico te verwaarlozen is."

Van de Looy beaamt wel dat het inzage hebben in broncode inzicht in de werking van software kan vergroten. "Vaak heb je bij het testen van een product op beveiligingsfouten door kennis en ervaring al het gevoel dat iets niet goed zit in een bepaald onderdeel. Op dat moment is het erg handig als je de sourcecode hebt, zodat je kunt zien hoe het probleem wordt opgelost. Maar het kan ook best zonder."