CHILLI: scanning tool externe netwerkkoppelingen

R.L. Moonen en drs. E.R. Nieuwland

'Tussen droom en daad staan wetten en praktische bezwaren.' Zelfs als de droom het handhaven van een wet of beleidsregel is, blijken de praktische bezwaren soms in de weg te staan. Een voorbeeld hiervan is het verbod op ongecontroleerde verbindingen van het bedrijfsnetwerk met het internet. Deze 'ongewenste intimiteiten' vormen een potentieel gevaar voor de veiligheid van het netwerk. Het is echter niet haalbaar continu fysieke controles uit te voeren en bestaande geautomatiseerde hulpmiddelen richten zich eerder op beheer dan op beveiliging. Een door de auteurs ontwikkeld tool spoort internet-koppelingen op en helpt daarmee de beveiliging van een netwerk (verder) onder controle te krijgen.

Inleiding

Inzet van internettechnologieën is vaak één van de voortvloeisels uit de strategie en het beleid van een bedrijf. Organisaties die hiervoor kiezen realiseren zich meestal al snel dat een (internet) beveiligingsbeleid een onmisbaar element is van die strategie. Dit kan onder meer tot uiting komen door een wildgroei aan (decentrale) ICT- en internetinitiatieven, die meestal een functionele drijfveer hebben en waarbij nogal eens aan de impact op de beveiliging voorbij wordt gegaan. Vooral in grotere en/of geografisch verspreide organisaties onttrekt een deel van dergelijke activiteiten zich aan het directe (toe)zicht van de terzake verantwoordelijke(n). Meestal beschikt dit management ook niet over voldoende competenties om zelfstandig vast te stellen welke externe koppelingen aanwezig zijn en in hoeverre ze worden gebruikt.

Een probleem hierbij is dat een aantal veelvoorkomende veiligheidsbepalingen tot op heden geen geautomatiseerde of tool-based controlemiddelen kende en dat het naleven van dergelijke bepalingen hierdoor soms geheel niet te controleren is, waardoor deze bepalingen moeilijk te handhaven zijn. Dit betreft onder meer bepalingen die te maken hebben met zelf geïnstalleerde software op desktop- en laptopcomputers, het gebruik van laptops in netwerkomgevingen anders dan het eigen kantoornetwerk en externe modem- en netwerkverbindingen vanaf het eigen kantoornetwerk. Wij zijn in de praktijk regelmatig geconfronteerd met de praktische vraag hoe dergelijke bepalingen te handhaven. Enige tijd geleden hebben we daarom een tool ontwikkeld voor de detectie van ongeautoriseerde internetkoppelingen.

R.L. Moonen
is werkzaam als manager bij KPMG Information Risk Management. Hij houdt zich bezig met de dienstverlening van KPMG met betrekking tot informatiebeveiliging, in het bijzonder het testen van de effectiviteit van technische beveiligingsmaatregelen.

moonen.ralph@kpmg.nl

Drs. E.R. Nieuwland
is werkzaam als manager bij KPMG Information Risk Management. Hij houdt zich bezig met de dienstverlening van KPMG met betrekking tot informatiebeveiliging, met name in de technische infrastructuur.

nieuwland.eric@kpmg.nl

Bedreiging van binnen uit

Tot op heden werden ongeautoriseerde internetkoppelingen niet als het meest acute probleem beschouwd. Immers, andere meer dringende zaken, zoals het creëren van een veilige internetkoppeling en e-mailinfrastructuur en het controleren en monitoren van internetgebruik, hadden een grotere prioriteit (figuur 1). Hiervoor zijn technieken en diensten ontwikkeld als wardials, penetratietests en configuratiereviews.
Echter, de tijd verandert, en daarmee ook de (beheersing van) risico's die gepaard gaan met internetgebruik en mobiliteit van gebruikers. Een risico dat in toenemende mate aandacht verdient, is het risico van ongeautoriseerde externe koppelingen. Hierbij moet u denken aan:

- gebruikers die naar internet uitbellen om de URL-blacklist[1] te omzeilen, terwijl ze tegelijkertijd een koppeling met het interne netwerk hebben;
- een afdeling die liever zelf een website host en daarom een eigen ADSL-lijn heeft genomen, maar ook aan het LAN gekoppeld is;
- foutief geconfigureerde VPN-tunnels, waardoor 'open uiteinden' naar het internet ontstaan.

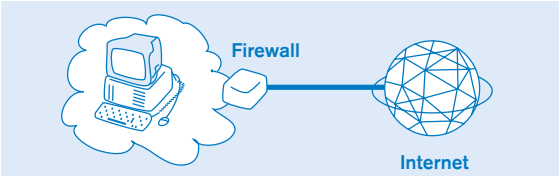
Soms zijn ongeautoriseerde externe koppelingen een erfenis van fusies of overnames. Het mag duidelijk zijn dat wanneer de voordeur goed op slot zit (firewall), de aandacht vervolgens gericht moet zijn op de achterdeuren (ongeautoriseerde externe koppelingen).

Zoals in figuur 2 wordt geïllustreerd, is het bestaan van dergelijke achterdeuren een aanzienlijk risico voor de beveiliging van het interne netwerk. Virussen, wormen, maar ook hackers kunnen via deze achterdeuren het interne netwerk binnendringen.

Wanneer een ICT-auditor gevraagd wordt een oordeel te geven over de ICT-beveiliging zal hij dus ook rekening moeten houden met eventuele onbekende en potentieel onbeschermde externe koppelingen. In veel gevallen wordt impliciet aangenomen dat het interne netwerk veilig is en worden er op centrale servers geen (aanvullende) maatregelen getroffen die passen bij een systeem met een directe, onbeschermde internetkoppeling. Het bestaan van dergelijke koppelingen heeft dan ook een enorme impact op het beveiligingsniveau.

Detectie

Het TCP/IP-protocol wordt tegenwoordig in vrijwel alle netwerken toegepast. In dit protocol worden berichten uitgewisseld door ze als één of meer gegevenspakketten van zender naar ontvanger te transporteren. Hiertoe worden de gegevenspakketten voorzien van een bestemming en, onder meer ten behoeve van het eventuele antwoord, een afzender. Niets weerhoudt ons er echter van een valse afzender te vermelden!



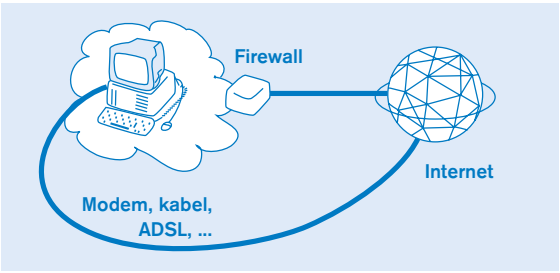
Figuur 1. Situatie zoals het hoort.

De genoemde achterdeuren blijken redelijk eenvoudig op te sporen, indien handig gebruik wordt gemaakt van het feit dat de TCP/IP-implementatie op de meeste computersystemen geprogrammeerd is om antwoord te geven op vervalste gegevenspakketten:

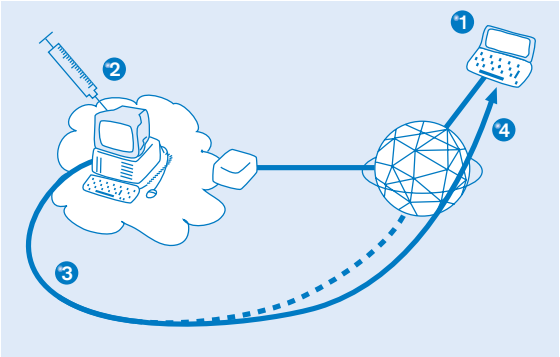
- *Stap 1.* Luister op internet naar gegevenspakketten vanuit het interne netwerk.
- *Stap 2.* Stuur vanaf het interne LAN een gegevenspakket met vervalst afzendadres (van de machine op internet, stap 1) naar de verdachte machine.
- *Stap 3.* De verdachte machine antwoordt op het gegevenspakket via de ongeautoriseerde verbinding met de buitenwereld.
- *Stap 4.* Als een antwoord wordt ontvangen, is een externe verbinding ontdekt.

Deze opzet werkt natuurlijk alleen onder bepaalde voorwaarden. Ten eerste dient het vervalste afzendadres het adres te zijn van de machine die op internet luistert, ten tweede dient het gegevenspakket er een te zijn dat inderdaad een antwoord genereert en ten derde moet de infrastructuur het verzenden van pakketten met vervalst afzendadres ondersteunen. Het blijkt in de meeste geval-

1) De door de firewall of proxyserver geblokkeerde websites.



Figuur 2. Realiteit: achterdeuren bestaan!



Figuur 3. Stappen in de detectie van een internetverbinding met behulp van vervalste gegevenspakketten.

len eenvoudig om aan deze voorwaarden te voldoen. Pakketten die hiervoor in aanmerking komen zijn:
- UDP-pakketten naar een gesloten poort (het antwoord hierop is een 'ICMP port unreachable'-pakket);
- ICMP echo request (beter bekend als 'ping')-pakketten (het antwoord is een 'ICMP echo reply');
- TCP SYN-pakketten naar een open poort (het antwoord hierop is een SYN/ACK-pakket);
- TCP SYN-pakketten naar een gesloten poort (het antwoord hierop is een RST-pakket).

Het is altijd mogelijk dat het interne netwerk de vervalste pakketten tegenhoudt of dat een ongeautoriseerde verbinding geen directe netwerkverbinding met het internet toestaat. Wellicht biedt de ongeautoriseerde verbinding dan een proxy-dienst aan. Deze koppelingen zijn te ontdekken door te zoeken naar bekende proxy-diensten. Proxy-diensten zijn meestal geconfigureerd om gebruik te maken van standaard TCP-poorten en verkeer naar deze poorten wordt meestal vrij doorgelaten door het interne netwerk. Door nu te controleren of deze poorten openstaan, en zo ja deze te verzoeken om bijvoorbeeld www.cnn.com te sturen, kan worden nagegaan of inderdaad sprake is van een proxy-dienst. Op deze manier wordt dan langs een andere weg het bestaan van de koppeling vastgesteld.

Door deze twee technieken te combineren is het mogelijk om geautomatiseerd alle 'hosts' op een netwerk te testen op externe koppelingen. De beschikbaarheid van hulpmiddelen om er deze tests mee uit te voeren is een grote stimulans gebleken voor de controle op externe koppelingen.

Wij hebben de hier beschreven techniek gestalte gegeven in de door ons ontwikkelde CHILLI-software (Centralised Hidden Internet Link Locating Infrastructure). Deze software bestaat uit drie elementen, te weten de zender van de vervalste pakketten, de ontvanger op internet en de rapportagemodule. Door periodiek de zender het gehele netwerk te laten scannen, kan in kaart worden gebracht waar zich internetkoppelingen bevinden. Verder onderzoek kan dan uitwijzen of dit geautoriseerde dan wel ongeautoriseerde koppelingen zijn. Op deze manier is er een geautomatiseerd hulpmiddel beschikbaar voor een actief externe-koppelingenbeleid.

Tijdens een scan met CHILLI op het netwerk van een zakelijke dienstverlener werd naast een bewust aangebracht controlepunt (ter bevestiging van de correcte werking) een onverwachte externe verbinding aangetroffen. Nader onderzoek wees uit dat een senior medewerker buiten de geboden beveiligingsfuncties om een verbinding naar het internet had gelegd. De interne organisatie heeft het incident verder afgehandeld.

In een ander onderzoek werden alleen de toegestane externe koppelingen aangetroffen. Blijkbaar waren er op het moment van de test geen ongeautoriseerde koppelingen actief die met onze testmethode gedetecteerd kunnen worden. De toegestane koppelingen hadden zich echter uit veiligheidsoverwegingen niet kenbaar mogen maken in de TCP/IP-test en dat was een reden om de configuratie aan te passen.

Conclusie

We hebben binnen de eerste versie van CHILLI een eerste set van mogelijke detectiemethoden gerealiseerd. Zelfs met deze beperkte set is het al mogelijk gebleken ongeautoriseerde koppelingen te vinden. Daarmee is aangetoond dat het met de juiste tools mogelijk is een begin te maken met het daadwerkelijk handhaven van een externe-koppelingenbeleid. Ondertussen ontwikkelen de auteurs deze detectiemethoden verder, deels binnen CHILLI, deels in andere software.

Literatuur

[Wolf00] Ir. R. de Wolf, *Infrastructure Services – Tool-based auditing in open heterogene ICT-infrastructuren*, Compact 2000/4.