Infoblad

‘RAT’tenplaag in het mkb

“RAT”: Remote Access Trojan, is een gemeen virus dat criminelen in staat stelt alles op een computer te volgen en geld weg te sluizen. Je bedrijf er tegen beschermen is echter goed mogelijk en hoeft niet moeilijk te zijn. Hieronder meer informatie, voor elke ondernemer met internet een must.

Wat is een RAT-aanval?

Cybercriminelen zijn creatief en verzinnen steeds nieuwe manieren om slachtoffers te misleiden en aan te vallen. Een nieuwe variant is de zogenoemde “Remote Access Trojan” (RAT). De cybercrimineel kan na een hack van de computer van de ondernemer grote sommen geld wegsluizen van zakelijke rekeningen. Dit type betalingsfraude lijkt zich vooralsnog op het mkb te richten.
De cybercrimineel verandert eén van de zakelijke rekeningnummers bij internetbankieren verandert in dat van hemzelf. De eigenaar maakte nietsvermoedend geld over naar deze rekening. Het gevolg: grote financiële schade. Dit had voorkomen kunnen worden met betere cybersecuritykennis van het bestaan van RAT’s.

Hoe komt een RAT-aanval tot stand?

In het algemeen begint een aanval met een e-mail waarin de crimineel de ondernemer of medewerker weet te verleiden op een link te klikken (phishing). Soms is het een algemene e-mail, vaak ook een mailing gericht op de specifieke sector zodat deze eerder serieus genomen wordt, geopend en of zelfs doorgestuurd binnen of buiten het bedrijf.
Wie de link aanklikt gaat naar een website waarin kwaadaardige inhoud (een computervirus, (RAT-)malware) verborgen is. Het virus weet zich te installeren op de computer omdat het misbruik maakt van fouten (bugs) in het besturingssysteem, de webbrowser of andere op de computer aanwezige software. Soms gaat het om nieuwe, nog onbekende kwetsbaarheden, vaker om fouten die al bekend zijn maar nog niet gerepareerd omdat de gebruiker software-updates niet direct doorvoert.

Het virus dat de crimineel nu heeft weten te installeren is onzichtbaar. Maar de dader kijkt vanaf dat moment ongemerkt mee, met alles wat wordt gedaan: elke toetsaanslag, elk bestand op de computer en het netwerk, elk wachtwoord dat wordt ingevoerd en ook welke betaling wordt uitgevoerd. De crimineel kan rustig een paar weken de tijd nemen om gedrag, gewoontes enz. te doorgronden en te ontdekken welke mogelijkheden er zijn om misbruik van te maken.

Als er voldoende informatie is verzameld wordt toegeslagen. Vaak gebeurt dit door betalingen te manipuleren. Bijvoorbeeld door rekeningnummers waar geld naar wordt overmaakt te wijzigen (al dan niet via het adresboek van de banktoepassing). Soms ook worden enkele extra betalingen klaargezet en de administratieapplicatie gemanipuleerd.
Wie niet héél scherp oplet en (drie)dubbel checkt, tekent vervolgens een banktransactie waarmee geld (winst, inkoop, continuïteit, reputatie) wordt weggesluisd naar de rekening van een crimineel.

Let wel; de bank ziet dergelijke overboekingen als volkomen normale opdrachten, door de ondernemer of financiële afdeling zelf getekende transacties en zal (kan) deze niet tegenouden.

Wat kun je doen tegen een RAT-aanval?

Om je te beschermen tegen de hierboven beschreven criminele tactieken zijn een aantal maatregelen mogelijk. Niet alleen technisch van aard, ook over de werkwijze van ondernemer en medewerkers.

Slimme medewerkers!

Houd beveiligingscodes geheim

- Licht medewerkers voor over de gevaren van het gebruik van internet en privé-email op de werkplek
- Klik nooit op links in e-mails zonder te weten waar de link naar verwijst. Houd eventueel uw muisaanwijzer stil boven de link; het mailprogramma zal laten zien hoe de volledige link er uit ziet
- Druk medewerkers op het hart om nooit op ongewone telefoonverzoeken in te gaan.

Controleer de bankrekening

- Controleer altijd de combinatie van namen en rekeningnummers van betalingen. Banken voeren geen controles uit op geldige naam/rekeningnummercombinaties
- Voer deze controle ook uit op de gegevens uit de adresboeken die worden gebruikt in de administratie- en bankapplicatie.
- Hanteer een vier-ogen principe; laat betalingen altijd door een tweede persoon controleren
- Sommige banktoepassingen ondersteunen ‘dubbele procuratie’. Dit houdt in dat altijd een extra persoon en bankpas-PIN-combinatie nodig is om de transactie digitaal te ondertekenen. Als de bankapplicatie deze functie ondersteunt, activeer deze dan en voer de extra procuratie bij voorkeur op een andere computer uit.

Zorg ervoor dat de bankpas nooit door een ander gebruikt wordt

- Laat nooit de bankpas (of ander door de bank verstrekt authenticatiemiddel) in een met de computer verbonden kaartlezer zitten. Zonder die pas kan de crimineel die de computer heeft overgenomen nooit zelfstandig een transactie verzenden en ondertekenen.

Meld incidenten direct aan de bank en volg aanwijzingen van de bank op

- Stop bij twijfel alle banktransacties en neem contact op met de bank

Voor de systeembeheerder: hoe voorkom en detecteer je een RAT?
Zorg voor een goede beveiliging van apparatuur die wordt gebruikt voor bankzaken

- Installeer altijd de updates voor alle software (zowel voor besturingssystemen als applicaties)
- Maak gebruik van antivirussoftware en werk deze regelmatig bij
- Scheid gewone werkplekken en financiële- en administratieve systemen, bij voorkeur in van elkaar gescheiden netwerken. Soms kan dit al eenvoudig door één computer exclusief voor bankverkeer te gebruiken
- Laat beheerrechten bij de systeembeheerder en niet bij alle medewerkers
- Houd logboeken bij van ingelogde gebruikers en gebruikte applicaties, en controleer deze regelmatig op afwijkend gedrag (bijvoorbeeld op nachtelijke activiteit).

En als het dan toch is misgegaan?

First things first!

1) Isoleer het besmette systeem door de netwerkverbinding te verbreken (verwijder de netwerkkabel en schakel de WiFi-verbinding uit). Laat het systeem aan staan
2) Bel vervolgens de politie (0800-8844) om aangifte te doen (zie verderop)
3) Waarschuw de bank en volg hun instructies op.

Nadat de politie klaar is met het onderzoeken van het systeem dient de systeembeheerder (of partij waar dit aan uitbesteed is) de volgende handelingen uit te voeren:

- Installeer het besturingssysteem van het besmette systeem opnieuw of vervang het volledig
- Controleer of andere systemen (computers en netwerkapparatuur) in hetzelfde netwerk besmet zijn, voer een volledige virusscan uit
- Controleer transacties en logboeken zorgvuldig.

Hoe doe je aangifte na een RAT-besmetting?

Het plaatsen van een RAT-tool, het binnentreden van andermans systemen, gebruik/misbruik maken van die systemen en het eventueel wegsluizen (stelen) van geld van een rekening is vanzelfsprekend strafbaar. Aangifte doen van het criminele feit (of feiten) bij de politie is daarom van groot belang. De politie maakt hiervan een proces-verbaal op.
De beslissing of daarna ook daadwerkelijk vervolging wordt ingesteld ligt bij het Openbaar Ministerie (OM). Bij aangifte doen is het voor de opsporing belangrijk dat gegevens, die herleidbaar zijn tot de criminele feiten, niet worden gewijzigd of aangepast. Dus: eerst aangifte en pas als de sporen zijn zeker gesteld opnieuw installeren.

Waarom is aangifte doen van belang?
Succesvol onderzoek doen naar daders begint met informatie van aangiftes. Die geven inzicht in de wijze van handelen van de crimineel of organisatie van criminelen. Als elk benadeeld bedrijf aangifte doet van de

besmetting wordt meer informatie verzameld en gecombineerd. Hoe meer informatie, hoe groter de kans dat op basis daarvan succesvol onderzoek kan worden gedaan naar de daders.

Aangifte doen is ook van belang voor het herkennen van nieuwe RAT's. De informatie uit de aangifte kan leiden tot aanpassingen in beveiligingssoftware, antivirusprogramma's en in updates van systemen. Dit maakt het voor alle mkb-bedrijven weer een stuk veiliger.

Tot slot: de verzekeringsmaatschappij zal een kopie vragen van de aangifte (mits verzekerd tegen cybercrime).

Voorbereid aangifte doen!
Aangifte doen van deze vorm van criminaliteit kan bij elk politiebureau. Vraag bij het maken van een afspraak om aangifte te doen altijd om de aanwezigheid van een digitaal rechercheur, dat helpt bij het formuleren van de aangifte en zorgt dat deze zo compleet mogelijk wordt opgenomen.
Bij het opnemen van de aangifte zal om informatie worden gevraagd die gebaseerd is op de wettekst en dus op de elementen van het strafbare feit, zoals:

- betreft het een aangifte tegen een particulier of een bedrijf?
- zijn er beveiligingsmaatregelen genomen?
- wat is de geschatte schade (uren in geld, immateriële schade) en wat zijn de herstelkosten?
- een beschrijving van de (technische) situatie
- is er al een verdachte bekend?

Voor meer informatie:

- Veiliginternetten.nl
- National Cyber Security Centrum NCSC
- Politie
- Fraudehelpdesk
- Veiligbankieren.nl
- De website van de bank.

Colofon

Dit infoblad is een uitgave van de
Koninklijke Vereniging MKB-Nederland,
Postbus 93002,
2509 AA Den Haag
T. 015-219 12 12
www.mkb.nl