Whitepaper

External Exposure

Remote toegang, patch/update, misconfiguraties

Leusden, 14 oktober 2021

Versie 1.0

Leusderend 38, 3832 RC LEUSDEN info@access42.nl www.access42.nl

Inhoudsopgave

1. External Exposure

Ruim 91% van de cyberaanvallen begint met een aanval over de email. In dit artikel bespreken we de meest voorkomende aanvallen die wij zien en die de overige 9% vormen. Deze overige aanvallen maken veelal gebruik van de zogenaamde External Exposure, hoe zichtbaar en kwetsbaar ben je als organisatie op het internet. Onderwerpen zoals Remote Desktop Protocol (RDP), patchen en misconfiguraties worden behandeld.

1.1 Remote Desktop Protocol

Remote Desktop Protocol (RDP) is een Microsoft Windows interface die een gebruiker in staat stelt om via het internet verbinding te maken met een andere computer of server en alle daarop geïnstalleerde tools en software. Naast RDP kennen we ook oplossingen als bijvoorbeeld Citrix. Allemaal technieken om op afstand toegang te krijgen tot systemen. Aangezien RDP een Windows-interface is, kunt u alleen verbindingen op afstand tot stand brengen met Windows PC's en Windows Server.

Waarom gebruiken bedrijven het? Om externe toegang tot een Windows machine mogelijk te maken. Hier zijn een paar veel voorkomende scenario's vandaag:

- Een IT-afdeling is niet langer in staat om werk uit te voeren op een laptop van een werknemer in persoon omdat iedereen op afstand werkt als gevolg van de pandemie.
- De netwerkschijven vertonen een storing en de servers die de schijven ondersteunen moeten worden benaderd en gepatcht om de schijven weer online te brengen.
- Medewerkers werken vanuit huis en nemen op kantoor “de desktop over” om het werk te kunnen doen.

In beide scenario's geeft RDP uw IT-afdeling of medewerkers toegang tot deze systemen alsof ze op kantoor zijn, zonder dat ze fysiek aanwezig hoeven te zijn.

1.2 RDP & Ransomware

In toenemende mate gebruiken kwaadwillende open RDP-poorten of remote toegang zoals Citrix (maar ook VPN) om toegang te krijgen tot systemen van een organisatie om ransomware te installeren. Ransomware is een soort malware waarmee gegevens van een organisatie worden versleuteld en vaak ook gestolen, waarbij wordt gedreigd de gegevens vrij te geven of de toegang te blokkeren totdat het slachtoffer losgeld betaalt. Vaak wordt er misbruik gemaakt door criminelen van eventuele kwetsbaarheden, of van accounts die gekocht of gelekt zijn. Er is vaak geen sprake van Multi Factor Authenticatie (MFA), dus naast het wachtwoord nog een extra manier om te authentiseren.

Een belangrijke oorzaak van de toename in RDP aanvallen is de migratie van werknemers van de werkplek naar de thuisomgeving als gevolg van de pandemie. Uit rapporten bleek dat het gebruik van RDP met 41% was gestegen sinds het begin van de pandemie, omdat bedrijven werken op afstand mogelijk maakten.

Stay secure

- Schakel RDP (of externe toegang) uit als uw bedrijf het niet gebruikt of niet nodig heeft. Vraag uzelf: Is toegang op afstand echt nodig binnen uw organisatie?
- Als je RDP nodig hebt, beperk het dan tot een gespecificeerde set van personen of IP-adressen die toegang hebben tot de RDP-poort. U kunt ongebruikte poorten ook sluiten na het voltooien van een taak of project.
- U kunt ook een Virtual Private Network (VPN) met multi factorauthenticatie (MFA) gebruiken. Microsoft stelt dat MFA meer dan 99,9 procent van de aanvallen om accounts te compromitteren kan blokkeren.

2. Patch management

Met patch management bedoelen we het up to date houden van de systemen en geïnstalleerde software. Iedere component die niet up to date is, is mogelijk kwetsbaar voor bestaande kwetsbaarheden. Criminele hackers kunnen misbruik maken van deze bekende kwetsbaarheden in besturingssystemen en services als deze niet goed zijn gepatcht.

Het snel patchen is essentieel voor effectieve cyberbeveiliging. Wanneer een nieuwe patch wordt uitgebracht, zullen aanvallers snel de onderliggende kwetsbaarheid in de applicatie identificeren en malware vrijgeven om deze uit te buiten. Als een criminele hacker met succes kan aanvallen voordat het doelwit de kwetsbaarheid heeft gepatcht, is de kans op inbreuk groot, met als mogelijk gevolg een datalek, ransomware of diefstal van bedrijfsgeheimen.

Stay secure

Patchen is een complex proces, omdat er meerdere IT-systemen bij betrokken kunnen zijn. Het implementeren van een patch kan ook het IT-landschap van een bedrijf destabiliseren. Daarom is het belangrijk om zo vroeg mogelijk te patchen, zodat u eventuele ernstige gaten in de software kunt repareren. Hoe langer u wacht met het installeren van de patch die nodig is, hoe groter de kans op een cyberincident.

- **Kies een regelmatig, terugkerend tijdstip voor het patchen**
  Het plannen van de patchingcyclus is essentieel. Kies een regelmatig en terugkerend tijdstip waarop patches moeten worden uitgevoerd. Zo voorkomt u dat systemen te lang niet worden bijgewerkt. Plan bijvoorbeeld een regelmatig onderhoudsvenster om alle laatste updates voor het besturingssysteem te installeren. Natuurlijk kunt u verschillende cycli instellen voor verschillende soorten patches. Dringende of kritieke patches zullen een andere aanpak vereisen dan regelmatige patches. Het traditionele patchen na de patch Tuesday van Microsoft is niet meer voldoende. Patchen is een dagelijks proces geworden. Kijk ook eens goed of sommige applicaties (bijv. Chrome) niet automatisch kunnen worden bijgewerkt.
- **Abonneer u op alle relevante mailinglijsten voor beveiliging**
  Dat betekent meer dan alleen Microsoft- of Linux-updates. Zorg dat je een overzicht hebt van alle software die in de organisatie wordt gebruikt, inclusief randapparatuur en IoT-apparatuur. Abonneer je op de relevante mailinglijsten voor deze software, zodat je altijd op de hoogte bent.
- **Vulnerability scanning & management**
  Een andere optie is om gebruik te maken van een dienst als Vulnerability Scanning en Management. Daarmee krijgt u een lopend overzicht van kwetsbaarheden, ook als er nog geen patch beschikbaar is, zodat u proactief de juiste actie kunt ondernemen.

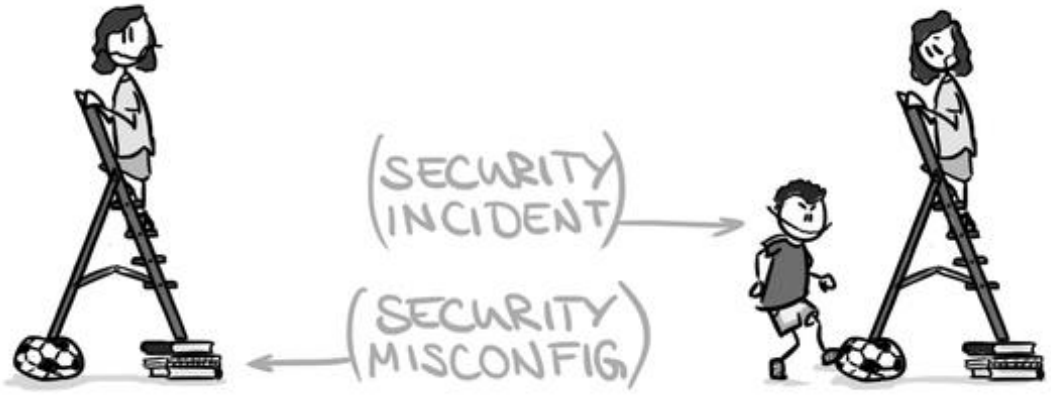
3. Misconfiguratie

Misconfiguraties worden vaak gezien als een gemakkelijk doelwit, omdat ze gemakkelijk te detecteren zijn op verkeerd geconfigureerde webservers, Cloud en toepassingen en vervolgens exploiteerbaar worden, aanzienlijke schade aanrichten en leiden tot catastrofale gegevenslekken voor ondernemingen. Zoals de blootstelling van Microsoft Power Apps in 2021. Hier zijn 38 miljoen dataentries van 47 overheids- en privacy bedrijven gelekt. Dit alles door een misconfiguratie in Microsoft Power Apps, een low-code service van Microsoft voor het bouwen van professionele toepassingen.

Misconfiguratie: Een gemakkelijke fout om te maken (en nog gemakkelijker te exploiteren)

Misconfiguratie is een brede term die veel terreinen kan bestrijken en op veel verschillende gebieden kan worden toegepast. Wat wel vaak voorkomt, is dat verkeerde beveiligingsconfiguratie optreedt wanneer de best practices niet worden gevolgd tijdens het instellen van beveiligingsmaatregelen voor een bedrijfsmiddel. De reden dat verkeerde configuratie wordt gezien als een kwetsbaarheid, is dat aanvallers zullen proberen deze fouten uit te buiten om ongeoorloofde toegang te krijgen tot het systeem van de gebruiker.

Een verkeerde configuratie van de beveiliging kan zowel op apparaten als op software betrekking hebben. Besturingssystemen, servers en applicaties kunnen allemaal worden getroffen. Hetzelfde geldt voor netwerkapparatuur, e-mailservers en eindgebruikersapparatuur zoals laptops of mobiele telefoons. Kortom, alles wat configureerbare beveiligingsfuncties heeft, kan ten prooi vallen aan deze kwetsbaarheid.



Stay secure

- **Beperk de toegang tot beheerdersinterfaces**
  Onderdeel van uw implementatiebeleid zou moeten zijn om beheerportalen uit te schakelen voor iedereen behalve voor bepaalde toegestane partijen. De uitvoering van het beleid moet ook worden gecontroleerd via regelmatige audits.
- **Verwijder ongebruikte functies.**
  Het enige wat ze uiteindelijk doen is je applicatie vatbaarder maken voor kwetsbaarheden door misconfiguratie. Als niemand ze zou moeten gebruiken, dan heeft het geen zin om ze te laten bestaan.
- **Vulnerability scanning & management**
  Maak gebruik van geautomatiseerde vulnerability management tools. Deze identificeren kwetsbaarheden binnen uw organisatie. Ook kwetsbaarheden die voortkomen uit misconfiguraties.