Opschrift

Vergadering van 9 september 2024

Nummer: 2024_MV_00385

Onderwerp:
Mondelinge vraag van raadslid Stephanie D'Hose: Ethisch hacken

Raadslid(-leden):
Stephanie D'Hose - Open Vld

Bevoegd: Sofie Bracke

Omschrijving van de vraag

Toelichting:
Cybersecurity is de laatste jaren een item waar we – terecht – veel aandacht aan schenken. Als stad beheren we namelijk heel wat gevoelige gegevens van burgers en bedrijven, waar we uiteraard omzichtig mee moeten omspringen. Het is daarnaast zo dat ook steden en gemeenten regelmatig geviseerd worden door hackers, met de bedoeling om systemen te blokkeren of gevoelige informatie te verkrijgen, en daarna losgeld te eisen.
Ethisch hacken is het principe waarbij hackers te goeder trouw de veiligheidssystemen van een bedrijf of organisatie testen. Merkt men daarbij slecht beveiligde gegevens op, programmeerfouten of andere mogelijke 'achterdeurtjes' waarlangs iemand met slechte bedoelingen zich toegang tot het systeem zou kunnen verschaffen, dan wordt dat gerapporteerd aan de organisatie in kwestie. Op die manier kan die zich wapenen tegen hackers, de continuïteit van haar dienstverlening garanderen en de gegevens van haar klanten veiligstellen.
Heel wat organisaties schakelen zelf ethische hackers in, met de vraag om hun systemen te onderzoeken op kwetsbaarheden. Ethische hackers mogen sinds vorig jaar ook spontaan proberen om Belgische organisaties te hacken, zolang ze de gevonden kwetsbaarheden maar zo snel mogelijk melden en er geen financiële voorwaarde aan koppelen.

Vraag:
Doet de stad beroep op ethische hackers om haar systemen aan een veiligheidscheck te onderwerpen? Zo ja, werden er op die manier al resultaten geboekt?
Werd de stad al door spontane ethische hackers gecontacteerd naar aanleiding van door hen opgemerkte issues?

Antwoord

Het is inderdaad zo dat sinds enkele jaren ethische hackers onze systemen spontaan onder de loep nemen. Dergelijke gemelde kwetsbaarheden werden steeds door District 09 bekeken en beoordeeld en indien nodig opgelost.
Verschillende meldingen bleken evenwel onterecht (vals positief) waardoor er veel tijd werd verloren aan het onderzoeken van deze meldingen.
Met de security nota in 2023 is beslist om het vrijblijvend karakter van deze manier van werken om te zetten in een gestructureerde aanpak en werd een externe partij aangesteld nl. Zerocopter, een bedrijf dat reeds ervaringen had in de publieke sector en bij lokale overheden. Met deze nieuwe werking zijn er al bepaalde kwetsbaarheden gedetecteerd en opgelost.
Het ethisch hacken gebeurt nu op 2 verschillende manieren:

- Via Responsible Disclosure en via 'Bug Bounty'

Bij **Responsible Disclosure'** kunnen ethische hackers vrijblijvend kwetsbaarheden melden
In de eerste 8 maanden van 2024 werden 18 kwetsbaarheden gevonden. 50% van de gemelde kwetsbaarheden zijn kritisch of high. 9 kwetsbaarheden zijn opgelost, 6 kwetsbaarheden zijn in behandeling bij D09. Daarnaast werden ook 5 dubbele kwetsbaarheden gemeld en 2 kwetsbaarheden werden tegengehouden door Zerocopter.
In het **Bug Bounty** programma gaan de ethische hackers gericht bepaalde toepassingen testen. Deze toepassingen zijn door District09 geselecteerd, worden eerst door Zerocopter getest, en zijn toepassingen met een hoger risico, die bv. gevoelige en persoonlijke info bevatten.
Deze toepassingen worden vrijgegeven op het Bug Bounty platform waar meer dan 1500 gescreende ethische hackers gaan testen. Ethische hackers worden vergoed als ze kwetsbaarheden vinden.
Deze manier van werken is medio 2024 gestart en heeft tot op heden nog geen nieuwe kwetsbaarheden opgeleverd.
Het ethisch hacken is uiteraard maar één van de vele maatregelen die we nemen voor meer cybersecurity. Het benadrukt wel het belang dat wij hechten aan creatief en proactief omgaan met bedreigingen. De gespecialiseerde kennis en expertise van ethische hackers zijn een waardevolle aanvulling op onze inspanningen om onze digitale infrastructuur te beveiligen.