IT-Defense 2023: Visionen und düstere Prognosen

Mikko Hyppönen von WithSecure legte in seiner Keynote mit dem Titel „Scorched Earth" am zweiten Konferenztag bemerkenswerte Ansichten zur Zukunft der KI dar.

Von Jörg Riether

Hyppönens radikale Zukunftsvision: Computer werden in fast allem besser als Menschen sein (Abb. 1).

Auf der IT-Defense 2023 reflektierte zunächst der finnische Sicherheitsexperte und Autor Mikko Hyppönen über die Vergangenheit, in der 1997 IBMs Deep Blue den seinerzeit amtierenden Schachweltmeister Garry Kasparov schlug. In seinen Augen ist die KI-Vision seitdem und bis heute gleichermaßen großartig wie angsteinflößend. Die Geschwindigkeit entwickele sich rasant und allein in den letzten sechs Monaten sei hier mehr passiert als in den letzten 30 Jahren zusammen, so Hyppönen.

Er führte als Beispiele den Text-zu-Bild-Generator Stable Diffusion sowie die Textgeneratoren und Dialogsysteme ChatGPT und Bard an. Seine Prognose mutet unerhört an: Schon in naher Zukunft würden Computer bessere Kunst als Menschen erschaffen. Computer würden die besseren Poeten, die besseren Musiker, die besseren Programmierer und die besseren Maler sein, so Hyppönen. Das, was Computer dann produzieren, würde die Menschen tiefer und intensiver berühren als das, was ein Mensch jemals zustande bringen könnte. Er würde diese Vorstellung hassen. Es ändere aber nichts an der Realität und genau so werde es kommen, dies sei für ihn klar. Mehr noch: Wenn die Entwicklung so weitergehe wie aktuell, könnten Computer in 100 Jahren menschliche Intelligenz stimulieren.

Enter **tenant id, domain name,** or **email**:

ix.de — Get information

Property	Value
Default domain	heisezs.onmicrosoft.com
Tenant name	Heise Medien GmbH & Co. KG
Tenant id	30b24132-0c65-4261-ac6f-79103eb03e71
Tenant region	EU
Seamless single sign-on (SSSO)	enabled
Certificate-based authentication (CBA)	N/A
Verified domains	19

Domain	Type	STS
1004.ha.trunk4teams.eu	Managed	
1004.sbc01.4direct-routing.de	Managed	
50-cent-und-gut.de	Managed	
ct.de	Managed	
ct-fotografie.de	Managed	
duf.de	Managed	
heise.de	Managed	
heise-regioconcept.ch	Managed	
heisezs.mail.onmicrosoft.com	Managed	
heisezs.onmicrosoft.com	Managed	
hinstorff.de	Managed	
ix.de	Managed	

Nestori Syynimaas Werkzeuge haben es in sich und können sowohl zur Informationssammlung in M365-Umgebungen, wie hier bei ix.de, als auch aktiv-offensiv benutzt werden (Abb. 2).

Gesprächige Tenants

Azure-AD- und Microsoft-365-Experte Nestori Syynimaa sprach über das Vertrauen in M365-Umgebungen. In diesem Zusammenhang stellte er seine eigenen Tools vor. Diese beinhalten neben diversen PowerShell-Abfragewerkzeugen auch ein Web-GUI (siehe ix.de/zyfa), das über öffentlich zugängliche Quellen zahlreiche Tenant-Informationen einsammeln kann. Dass diese durchaus detailliert sein können, zeigt ein Versuch des Autors mit der Domain ix.de (Abbildung 2).

Es offenbart sich auf einen schnellen Klick, dass ix.de zur M365-Standarddomain heisezs.onmicrosoft.com gehört, die in der EU-Region beheimatet ist, außerdem gibt es im Tenant 19 verifizierte Domänen. Darunter gibt es auch Einträge wie „1004.ha.trunk4teams.eu", „50-cent-und-gut.de" sowie „heisezs.mail.onmicrosoft.com". Die Seamless-Single-Sign-on-Technik (SSSO) ist aktiviert und zertifikatbasierte Authentifizierung (Certificate-based Authentication, CBA) ist nicht vorhanden, dies kann man mit einer gültigen Mailadresse optional prüfen.

Dieses Beispiel ist noch relativ harmlos. Spannend ist, dass all diese Informationen „per Design" öffentlich verfügbar sind. Es lohnt sich, mit dem Werkzeug selbst ein wenig mit der eigenen Unternehmensdomain oder anderen bekannten Domains zu spielen. Man könnte das Tool auch dazu missbrauchen, valide Mailadressen herauszufinden. So gab das Web-GUI im Test bei einer vermutlich gültigen Microsoft-Mailadresse aktivierte CBA an, während es bei einer erfundenen Mailadresse aus vielen zufälligen Zeichen „nicht vorhanden" ausgab. Es lassen sich also möglicherweise mehr Informationen ableiten, als dem einen oder anderen Unternehmen lieb sein könnte.

Auch die PowerShell-Werkzeuge sind mächtig. Neben der passiven Informationsbeschaffung gibt es hier sogar ein Phishingmodul, mit dem man live einen Angriff durchführen kann, der einen bei Erfolg direkt ins Outlook Web Access des Opfers führt. Syynimaa macht sich hier die Azure Device Code Authentication zunutze (siehe ix.de/zyfa).

Aus dem Tesla-Nähkästchen

Der IT-Sicherheitsforscher Martin Herfurt stellte in seinem Vortrag Details zum Projekt TEMPA vor, das Werkzeuge und Details zum proprietären VCSEC-Protokoll bereitstellt. Gewonnen hat er diese Informationen durch Analyse der dekompilierten offiziellen Tesla-Android-Anwendung – und konnte so Einblicke in die Angreifbarkeit des Protokolls und damit des Fahrzeugs erhalten (mehr Details siehe ix.de/zyfa).

Herfurt berichtete, dass er die Relay-Verwundbarkeiten, über die mit zwei Raspberry Pis und Telefonen ein Tesla entwendet werden konnte (siehe ix.de/zyfa), an den Hersteller gemeldet hatte. Tesla ließ verlauten, dass man dies nicht ändern werde und die Kunden doch bitte PIN2Drive einsetzen sollen, also eine zusätzliche PIN-Abfrage, bevor man das Fahrzeug starten kann. Dazu rät auch Herfurt, denn leider seien die Relay-Angriffe auf Teslas immer noch sehr einfach möglich. (ur@ix.de)