secorvo
security consulting

Secorvo Security News

September 2022

Androide Gegner

Noch sind sie nicht die Regel, aber vereinzelt dürften sie bereits vorkommen: mit künstlicher Intelligenz optimierte Angreifer.

Das wachsende Angebot Cloud-basierter – also schnell und kostengünstig skalierbarer – KI-Systeme bietet immer mehr leistungsfähige Möglichkeiten, Angriffe auf IT-Systeme mit maschinellem Lernen zu verbessern.

Dass Angreifer die Suche nach bekannten Schwachstellen mit Crawlern automatisieren, ist lange bekannt. Auch die mühsame manuelle Suche nach Schwächen in der Eingabe-Validierung von Web-Anwendungen wird seit vielen Jahren mit Fuzzy-Systemen maschinell unterstützt.

Doch inzwischen könnten KI-Systeme auch gänzlich neue Schwachstellen identifizieren – vorausgesetzt, man würde sie mit geeigneten Samples „füttern". Ist der Source Code (wie z. B. bei Open-Source-Lösungen) zugänglich, funktioniert das zumindest im Labor.

Aber auch herkömmliche Angriffsmethoden lassen sich mit KI-Systemen perfektionieren. So können „Textgenerierungs-KIs" bereits heute beispielsweise an den Stil eines bestimmten Absenders adaptierte E-Mails formulieren, die von dessen eigenen nicht zu unterscheiden sind (siehe SSN 8/2022). Ein ideales Hilfsmittel für Spear-Phishing-E-Mails – und eine perfekte Methode, um CEO-Fraud zu optimieren. Schlimmer noch: Mit Stimm-Samples eines CEO trainiert kann ein KI-gesteuerter Sprachgenerator (siehe SSN 10/2020) einen täuschend echten Anruf des CEO vorspielen, sodass selbst engste Mitarbeiter die Falle nicht erkennen. Ganz ähnlichen Angriffen sehen sich heute biometrische Authentifikationsverfahren ausgesetzt. KI-Systeme können Bilder, Videos oder auch Fingerabdrücke erzeugen, die sich von echten nicht unterscheiden lassen.

Auch wenn KI-Systeme den Turing-Test noch nicht bestehen – in der Hand von Angreifern sind sie bereits ein gefährlicher Gegner.

Inhalt

secorvo
security consulting

Security News

Bug-Bounty-Marketing

Finden Forscher Schwachstellen in Software-Produkten, so erfolgt oft eine „responsible disclosure", sprich: eine Vorab-Benachrichtigung des Herstellers, die diesem Zeit einräumt, die Schwachstelle vor der Veröffentlichung zu beheben. Nach Ablauf dieser Karenzzeit werden Ursache und Auswirkungen der Schwachstelle meist als CVE (Common Vulnerabilities and Exposures) veröffentlicht. Um Nutzer der Software vor der Schwachstelle zu warnen, erfolgt die Veröffentlichung auch dann, wenn der betroffene Hersteller nicht reagiert hat. Inzwischen wird die Suche nach Schwachstellen von einigen Unternehmen durch Bug-Bounty-Programme gefördert: Wer eine Schwachstelle meldet, erhält eine kleine oder auch etwas größere Prämie. Das ist erstmal alles nicht neu (siehe SSN 12/2019).

Findet man zu einem Produkt wenige oder sogar keine CVEs, so kann das bedeuten, dass sich noch niemand die Mühe gemacht, es zu untersuchen. Bei verbreiteten Produkten ist es aber wahrscheinlicher, dass keine (oder nur wenige) Schwachstellen gefunden werden konnten – und das spricht für die Qualität des Produkts.

Wie die Forscher von modzero am 22.08.2022 veröffentlichten, gibt es allerdings noch eine dritte Möglichkeit: Jemand hat das Produkt untersucht, Schwachstellen festgestellt, sie dem Hersteller gemeldet, eine Prämie erhalten – sich aber über die Bestimmungen des Bug-Bounty-Programms verpflichtet, keine CVE zu veröffentlichen. Das Fehlen von CVEs sagt daher inzwischen leider wenig über die Sicherheit eines Produktes aus – Bug-Bounty-Programme als irreführendes Marketing…

Nmap-Jubiläum

Unglaublich, aber wahr: Nmap, der wohl bekannteste Netzwerk-Portscanner („Network Mapper"), wird 25 Jahre alt. Damit ist Nmap eines der (wenn nicht das) am längsten fortlaufend gepflegte Werkzeug für IT-Sicherheitsfachkräfte, Netzwerker und Administratoren. Die Entwicklung vom einfachen Portscanner über die Erkennung von Diensten und Betriebssystemen bis zur Bedienung über eine grafische Oberfläche – die Liste der Erweiterungen im Changelog ist lang. Nach wie vor kann man performant komplette Netzbereiche durchforsten und so bekannte und ggf. auch nicht zuzuordnende IT-Systeme und Netzwerk-Dienste finden.

Mit Nmap gelingt das genauso zuverlässig (und kostenlos) auch in der OT (Operational Technology) – zur Identifikation von im Netz erreichbaren Systemen muss man auch heute keine komplexen und kostspieligen Werkzeuge beschaffen. Wer wissen will, welche Systeme und Dienste in den eigenen Netzen – seien es Leittechnik oder Bürokommunikation, die DMZ oder der „Blick" vom Internet auf das eigene Netz – dem empfehlen wir der Einsatz von Nmap. Wir gratulieren, Fyodor!

Missbräuchliche Abmahnungen

Seit August erfasst eine Abmahnwelle Unternehmen und Privatpersonen in Österreich und Deutschland, die auf ihren Webseiten bei Google gehostete Fonts eingebunden haben. Darin werden – mit Bezug auf das Urteil des LG München (siehe SSN 6/2022) – Schadensersatzforderungen in Höhe von 100-200 € nach Art. 82 DSGVO geltend gemacht.

Tatsächlich sind die Schadensersatzansprüche in den meisten Fällen unbegründet, da der Anspruchsteller zur Ermittlung des Einsatzes von Google Fonts einen WebCrawler nutzt und die Abmahnungen automatisiert verschickt. Der Anspruchsteller war demnach nie persönlich auf den Webseiten, womit der Tatbestand des Art. 82 Abs. 1 DSGVO nicht erfüllt ist, da er nicht als natürliche Person betroffen war; die Schadensersatzforderung selbst erfolgt rechtsmissbräuchlich. In Österreich erstatteten daher Anwälte von Betroffenen Anzeige wegen gewerbsmäßigen Betrugs.

Der Fall zeigt, dass man beim Erhalt von Abmahnungen nicht vorschnell einen geforderten Schadensersatz direkt begleichen sollte. Wir empfehlen in einem solchen Fall Ruhe zu bewahren, zunächst die Begründetheit des Anspruchs genau zu prüfen und ihn gegebenenfalls zurückzuweisen.

Davon unbenommen sollte man allerdings auf der eigenen Webseite verwendete Google Fonts tatsächlich nicht einbinden, sondern auf dem eigenen Server hosten – Anleitungen dafür und hilfreiche Tools finden sich zahlreich im Internet.

Déjà-vu

Am 12.09.2022 stellte Martin Rost auf der Sommerakademie des ULD Schleswig-Holstein Neuerungen beim Standard Datenschutzmodell (SDM) sowie die Ergebnisse einer Umfrage zur Nutzung des SDM vor. Die wichtigste (und begrüßenswerte) Neuerung: Im Baustein 41 wurde eine aus dem IT-Grundschutz stammende Soll-Ist-Prüfung aufgenommen. Die in der Umfrage geäußerten Erfahrungen der Nutzer des SDM decken sich allerdings mit unseren Praxiserfahrungen: Es ist sehr aufwändig, die beschriebenen Maßnahmen zu prüfen und umzusetzen.

Das klingt nach einem déjà-vu. Im Jahr 2018 hatte das Bundesamt für Sicherheit in der Informations-

technik (BSI) aus denselben Gründen nach 15 Jahren die umfänglichen Maßnahmenvorschriften im IT-Grundschutz-Katalog auf Anforderungen an die Informationssicherheit in Form des IT-Grundschutz-Kompendiums umgestellt. Das BSI hatte (endlich) erkannt, dass Betreiber von Managementsystemen die operative (und unternehmerische) Freiheit benötigen, risikobezogen über Maßnahmen und deren Umsetzung zu entscheiden.

Im CON.2-Baustein des IT-Grundschutz-Kompendiums referenziert das BSI auf das SDM, aber es hat wohl geahnt, dass man Unternehmen besser nicht zur Umsetzung zwingt. Ein weiser Schritt, denn es gibt auch andere, kostengünstigere Wege, ein wirksames Datenschutz-Managementsystem (DSMS) aufzubauen, als alle Gewährleistungsziele mit Maßnahmenbergen zu erschlagen. Die Vorgehensweise nach dem SDM ist grundsätzlich gut, allerdings sollten die Bausteine wie beim „neuen" Grundschutz praxistauglicher gestaltet werden.

Falsch verstandene Transparenz

Seit dem 01.08.2022 sind die Inhalte des „Gemeinsamen Registerportals der Länder" kostenfrei abrufbar. Das ist das Ergebnis der unmittelbaren Anwendung der „Digitalisierungsrichtlinie" der EU (Richtlinie 2019/1151) vom 20.06.2019 durch das Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG). Dem Inkrafttreten folgte ein „Aufschrei", weil nun über das Registerportal auch Dokumente eingesehen werden können, die zuvor nicht ohne weiteres zugänglich waren – wie die Privatadressen von Unternehmern, Geschäftsführern und Aufsichtsräten oder deren gescannte Unterschriften. Frei verfügbare Daten, die geradezu zum Missbrauch einladen.

Ziel der Digitalisierungsrichtlinie ist es, digitale Unternehmensgründungen zu vereinfachen und durch Transparenz Missbrauch und Betrug vorzubeugen. Klare Vorgabe des Gesetzgebers ist es, dass dabei die Grundsätze des Datenschutzes nach der DSGVO zu berücksichtigen sind. Bei der deutschen Umsetzung ist das zumindest teilweise schiefgegangen, da die beteiligten Registergerichte offensichtlich keine Interessenabwägung zwischen den schutzwürdigen Interessen der Unternehmer und der Sicherstellung von Vertrauenswürdigkeit durch Transparenz vorgenommen haben.

Fein raus sind lediglich Unternehmen, die ihre Dokumente vor dem 01.01.2007 eingereicht haben – die liegen nicht digital vor und sind daher auch nicht online abrufbar. Es ist zu hoffen, dass die Regelung einer Überprüfung unterzogen wird.

Secorvo News

Teamverstärkung

Seit dem 01.09.2022 verstärkt uns Oliver Oettinger in den Sicherheitsthemen Public Key-Infrastrukturen und Forensik. Herzlich willkommen im Secorvo-Team!

T.I.S.P. und BSI Vorfall-Experte

In der Woche **14.–18.11.2022** bieten wir Ihnen mit dem T.I.S.P.-Seminar die letzte Gelegenheit in diesem Jahr zur Zertifizierung Ihrer Kenntnisse in der IT-Sicherheit. Nach Eingang Ihrer Anmeldung erhalten Sie das von Secorvo verfasste Begleitbuch zum T.I.S.P. zur Vorbereitung auf das Seminar und die anschließende Prüfung. Wir empfehlen eine baldige Anmeldung.

Unser letztes Seminarangebot in diesem Jahr ist die Vorbereitung auf die Zertifizierung zum BSI Vorfall-Experten nach dem Curriculum des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der Kalenderwoche 48 (**29.11.–01.12.2022**). Wir freuen uns auf Ihre Anmeldung!

Die Seminar-Programme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Webseite unter https://www.secorvo.de/seminare.

Gotcha.

Das Nachverfolgen oder das Erstellen von Profilen zu Besuchern von Webseiten mittels Cookies ist bekannt und bekommt öffentliche Aufmerksamkeit – bei E-Mails haben Tracking und Profiling hingegen bisher kaum Aufmerksamkeit erfahren, obwohl diese bei Newslettern und deren Inhalten regelmäßig angewendet werden.

Auf dem kommenden Online-Event der KA-IT-Si am 03.11.2022 stellen Milan Burgdorf und Christian Blaicher (Secorvo) exemplarisch die technischen Möglichkeiten und Umsetzungen für Tracking und Profiling in E-Mails vor und beleuchten die rechtlichen Rahmenbedingungen für deren Verwendung. Wir freuen uns auf Ihre Teilnahme.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
November 2022	
07.-11.11.	ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US)
09.-10.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
14.-18.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
29.11.-01.12.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
Dezember 2022	
05.-08.12.	Black Hat Europe 2022 (Blackhat, London/UK)

Fundsache

Die Landesdatenschutzbeauftragte für den Datenschutz Niedersachsen hat im August 2022 FAQ zur Auftragsverarbeitung nach Art. 28 DSGVO veröffentlicht, die auf 15 Seiten lebensnahe Antworten zu Fragen rund um AV-Verträge geben.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de