Künstliche Intelligenz, Darknet und OSINT im Social Engineering

Stefan Loubichi

Abstract

New dimensions in social engineering

Social engineering is a method of obtaining security-relevant data by exploiting human behaviour. In the process, the criminal selects the person as the weak link in the security chain to put his criminal intentions into action. Criminals exploit human characteristics such as trust, helpfulness, fear, or respect for authority to manipulate these people.

In social engineering attacks, the focus is on the central feature of deception about the identity and intention of the attacker. Ever since life-threatening orders were issued by strangers in "deep fake" meetings during Ukraine war, or the mayor of Berlin only realised after 30 minutes that she was not talking to Kyiv mayor she knew, it has become obvious that there are new forms of "social engineering".

Deep Fakes bei KRITIS Betreibern – erstmalig 2019

In einer britischen Niederlassung einer deutschen Unternehmung klingelt an einem Freitag im März 2019 um 16 Uhr, d.h. kurz vor Feierabend das Telefon. Der große Chef der Konzernzentrale bittet darum, schnell 220.000 Euro an einen Lieferanten in Ungarn zu überweisen [1]. Es drohe eine riesige Vertragsstrafe und man könne nur noch schnell von Großbritannien aus überweisen, um dies zu verhindern. Natürlich würde das Geld umgehend am Montag von der Konzernzentrale in Deutschland an die Niederlassung in Großbritannien überwiesen. Die Stimme des Konzernchefs war bekannt, gleichwohl besteht die Niederlassung in England auf einer E-Mail-Bestätigung, welche prompt kommt. Das Geld wird sofort nach Ungarn überwiesen. Am Montag wurden jedoch keine 220.000 Euro aus Deutschland an die Firma in Großbritannien überwiesen, denn der Konzernchef hatte nie angerufen [2]. Die Stimmenimitation wurde realisiert mit der Software Lyrebird. Und bereits am 14.9.2018 hatte der Deutschlandfunk ausführlich über Lyrebird berichtet [3] …

Auf der diesjährigen vgbe Konferenz KELI "Elektro-, Leit- und Informationstechnik in der Energieversorgung" vom 10.-12. Mai 2022 hielt der Verfasser dieses Artikels einen Fachvortrag genau über dieses Thema: "Wie Cyberkriminelle die Identität einer Führungskraft der Kritischen Infrastruktur annehmen und was man gegen Social Engineering tun kann." [4]. Das Interesse am Vortrag war sehr groß – die Verwunderung des Vortragenden darüber, dass diese Form der Deep Fakes nicht bekannt war, war ebenfalls sehr groß.

Geld ist zu ersetzen, auch wenn 220.000 Euro nicht aus der Portokasse zu zahlen sind. Schlimmer wird es, wenn nicht der Konzernchef vermeintlich anruft, sondern ein vermeintlicher Anruf von BSI, Bundesnetzagentur oder der Cyberabwehr des Verfassungsschutzes erfolgen würde und man darum bittet, wegen einer sehr ernsten Bedrohungslage schnell einmal ….. Diese Folgen sollten wir uns gar nicht erst ausmalen. Wie schwierig ist dies aber alles?

Maschinelles Lernen – Grundlagen für deep fakes

Maschinelles Lernen (ML) ist ein Segment der Künstlichen Intelligenz, welche Systeme in die Lage versetzt, automatisiert aus Daten zu lernen und sich (kontinuierlich) zu verbessern, wobei eine Programmierung nicht erforderlich ist (vgl. Bild 1).

ML beginnt mit einem so genannten vorbereiteten Datensatz (=Trainingsdatensatz), wobei der Datensatz von einem ML Algorithmus nach Mustern und Zusammenhängen durchsucht wird.

Es liegt ein interaktiver Prozess vor, der so oft durchlaufen wird, bis das Ergebnis eine hinreichende Qualität erreicht hat. Die Ergebnisse aus dem ML Algorithmus müssen dabei von Menschen bewertet werden.

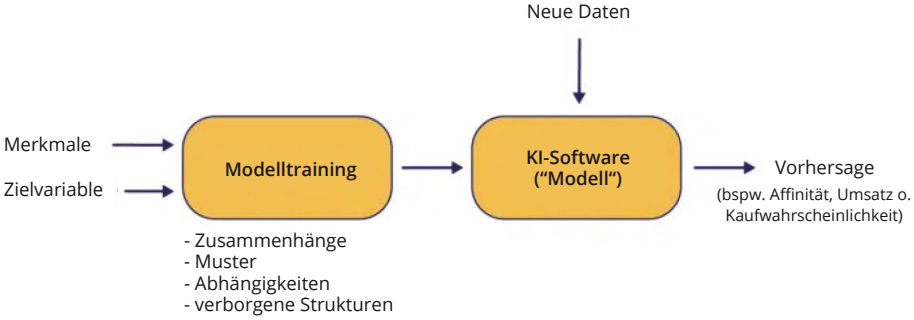


Bild 1. Funktionsweise von Maschinellem Lernen; Quelle: https://datasolut.com/was-ist-machine-learning/

Autor

Prof. h.c. PhDr. Dipl.-Kfm./Dipl.-Vw. Stefan Loubichi
Essen, Deutschland

Folgende Arten von Machine Learning Algorithmen gibt es:
- Überwachtes Lernen
- Unüberwachtes Lernen
- Teilüberwachtes Lernen
- Verstärkendes Lernen

Sollen ML Modelle Zusammenhänge finden, so bedarf es hierzu vorab eines Trainings. Dabei werden die nachfolgenden vier Schritte durchlaufen:
- Es werden dem ML Algorithmus von einem Menschen „Trainingsdaten“ zur Verfügung gestellt.
- Diese Daten werden von dem ML Algorithmus nach Mustern untersucht.
- Sobald der Trainingsprozess abgeschlossen ist, liegt ein sicheres Modell vor.
- Abschließend kann das ML Modell dazu verwendet werden, unbekannte Daten zu analysieren und auszuwerten.

An dieser Stelle sei am Rande darauf verwiesen, dass bereits vor 24 Jahren von der NATO über Neurale Netze und Maschinelles Lernen entsprechend informiert wurde, so dass hier nichts grundlegend Neues vorliegt [5].

Die für uns relevante Teilmenge des Machine Learning ist das Deep Learning (DL). DL „imitiert“ das menschliche Lernverhalten unter Zuhilfenahme großer Datenmengen.

Zwischen Künstlicher Intelligenz, Machine Learning und Deep Learning besteht dabei folgende Korrelation:

Oberbegriff:	Künstliche Intelligenz (KI) Software und Programme, die Probleme allein lösen können.
Mittelbegriff:	Machine Learning (ML) Teilgebiet der KI – Algorithmen, die von Daten lernen können
Unterbegriff:	Deep Learning (DL) [6] Teilgebiet des ML–Einsatz von tiefen, neuronalen Netzen

Bei sehr komplexen Mustern wie unstrukturierter Bild- und Texterkennung ist das Erlernen komplexer Muster mit klassischen ML Algorithmen nur schwer möglich. Hier bedarf es in der Regel künstlicher neuronaler Netze, wobei zur Bilderkennung gerne und sehr häufig Convolutional Neural Networks (CNN) eingesetzt werden.

Zum besseren Verständnis wird hier auf die frei downloadbare Vorlesung der Stanford Universität in Sachen CNN verwiesen [7]. Zur Funktionsweise wird bei DL Sichtweise auch auf die Grafik der Stanford Universität verwiesen, Bild 2:

In Sachen Bildverarbeitung wird darauf verwiesen, dass CNNs im Jahr 2016 eine Fehlerquote von 0,23 % auf eine der am häufigsten genutzten Bilddatenbanken, MNIST, erreichten, was der geringsten Fehlerquote aller jemals getesteten Algorithmen entspricht.

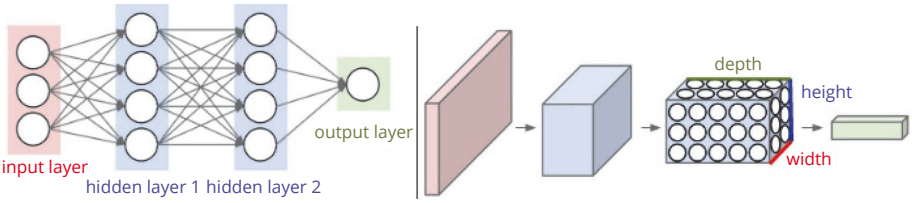


Bild 2. 3-layer Neural Network vs. Conv-Net ; Quelle: Kurs CS231n: Deep Learning for Computer Vision, Stanford University

Deep learning leicht gemacht – am Beispiel von Deep Face Lab u.a.

Bei dem von jedem zu einem günstigen Preis kaufbaren Programm Deep Face Lab, welches mit einer permanenten Wiederholung des Schemas Try and Error arbeitet, werden viele aufeinanderfolgende Schichten ausprobiert. So mag es zum Beispiel sein, dass die erste Schicht danach schaut, welche Farbe die wahrscheinlichste ist an der Stelle, wo der Mund ist. Die nächste Schicht schaut sich dann die Umgebung neben dem Mund an und so geht es dann Stück für Stück weiter. Deep Face Lab lernt mittels numerischer Werte, was ein spezielles Gesicht ausmacht, d.h.: Kopfhaltung, Ausdruck, Mimik. Es entsteht somit ein neuer Videoschnitt, jedoch künstlich generiert.

In der medialen Darstellung wird oft erklärt, dass dies nur dann machbar sei, wenn man ein so genanntes vortrainiertes Modell hat, wie es in der Regel bei Personen des öffentlichen Lebens ist. Dies stimmt nicht.

In einem solchen Fall muss das Programm lernen, ein beliebiges Gesicht in Zahlen zu übersetzen und diese Zahlen wieder in ein Gesicht zu übersetzen. Natürlich braucht man Zeit und Geld. Die Leistung eines guten Grafikprozessors (z.B. die NVIDIA Grafikkarte mit CUDA Unterstützung (mindestens GTX 1010) sowie drei bis vier Gigabyte Festplattenspeicher reichen zum Beispiel aus, dass mit der aus den Sozialen Medien bekannten Desktop Anwendung FakeApp mittels FaceSwap täuschend echt aussehende gefälschte Videos mit den Gesichtern anderer Menschen erstellt werden. [8].

Wer die Hintergründe auch noch verstehen möchte, der sei auf die in Youtube zu findenden Erklärvideos zum Thema Real Time Facial Reenactment verwiesen [9].

Eine weitere von Deep Face Lap genutzte Technik des Maschinellen Lernens ist „Generative Adversarial Networks (GAN) [10]. Diese – seit 2014 bekannte Technologie – lässt sich einfach erklären: In einer Art Wettstreit treten zwei neuronale Netzwerke gegeneinander an: Das eine Netzwerk versucht das Modell eines perfekten Gesichtes zu errechnen. Das andere Netzwerk versucht, entsprechende Fehler zu finden. Hiermit hat man die Büchse der Pandora geöffnet. Leider finden sich im Übrigen nur wenige Publikationen darüber, wie Deep Fake entdeckt werden kann [11].

Seit 2019 gibt es hier im Übrigen eine bahnbrechende Weiterentwicklung von Forschenden der Universität Trient aus Italien: First Order Motion Model for Image Imagination [12]. Bei Frist Order Motion wurden Erscheinungs- und Bewegungsinformationen durch eine selbstüberwachte Formulierung entkoppelt. First Order Motion Model berechnet aus einem statischen Foto, wie sich das Gesicht beim Sprechen bewegen würde und fügt eigene Bildteile ein. Die Fehlerrate ist zwar größer als bei „klassischen Deep Learning, aber immer noch hinreichend, um bei kleinen Videosequenzen zu überzeugen.

Avatarify Desktop ist im Übrigen eine im freien Handel erhältliche Software, die auf dem First Order Motion Model aufbaut.

Auf die umfangreiche Veröffentlichung des aktuellen Wissenschaftsstandes in NeurIPS Proceedings wird an dieser Stelle ausdrücklich verwiesen [13].

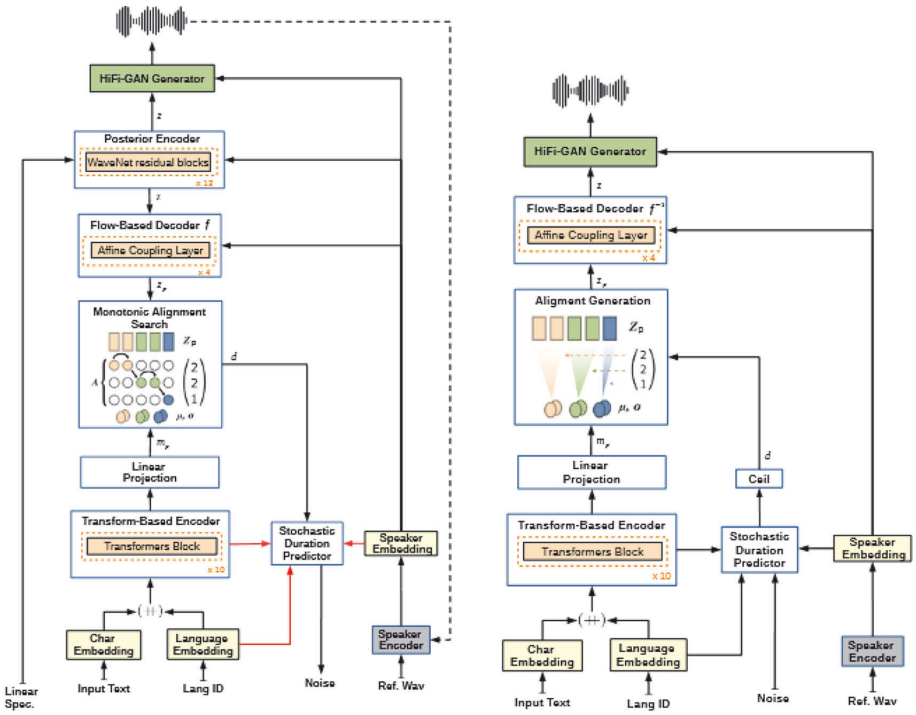
Kommen wir nun Problem mit der Stimmimitation. Hier sind die Produkte von Adobe, Adobe VoCo [14] und Baidu, Deep Speech [15] zu nennen. Während Adobe VoCo bis heute nicht kommerziell vermarktet wird, ist Baidu den Open Source Weg gegangen.

Voice Conversion Programme (Bild 3) gehen hierbei in der Regel nach folgendem Schema vor:
- Analyse des gesprochenen Wortes
- Zerlegung der Stimme des Sprechers in einzelne Phoneme
- Texteingaben werden in Realtime mit der Stimme des Sprechers synchronisiert.

Wie gut diese Systeme mittlerweile geworden sind, zeigen die Demoversionen der nachfolgenden im freien Markt erhältlichen Produkte (Bild 4), wobei hier nur einige genannt werden:
- https://www.descript.com/
- https://www.descript.com/lyrebird
- https://replicastudios.com/
- https://www.resemble.ai/
- https://www.respeecher.com/

Die große Frage ist dabei oftmals: Aber wie groß muss denn die Dauer einer Sprachaufnahme von jemandem sein, damit man dessen Sprache clonen kann [16].

DeepVoice benötigt zum Beispiel nur noch eine Sprachaufnahme von 3,7 Sekunden, um eine Stimme nahezu perfekt zu clonen. Diese Zahlen sind erschreckend.



(a) Training procedure (b) Training procedure

Bild 3. YourTTS diagram depicting (a) training procedure and (b) inference procedure, Quelle: https://arxiv.org/pdf/2112.02418v3.pdf

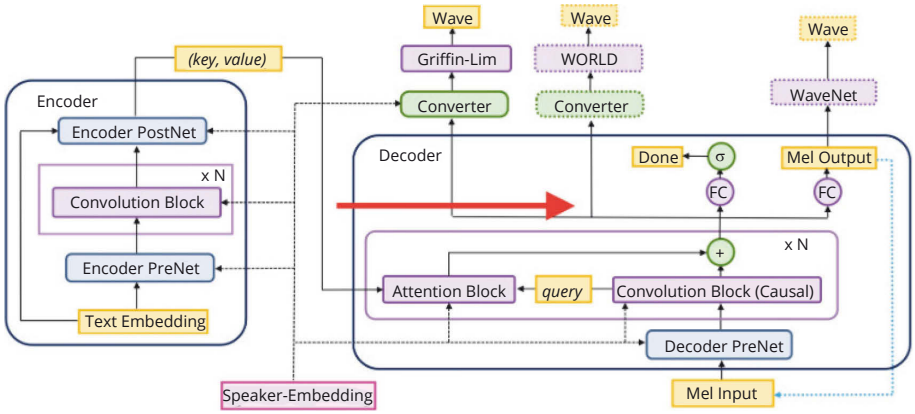


Bild 4. Architektur von Baidus Deep Speech 3, Quelle: http://research.baidu.com/Blog/index-view?id=90

Mittlerweile stehen die Grundlagenwerke hierzu auch der Öffentlichkeit in hinreichendem Umfang zur Verfügung [17].

Das Darknet

Viele verlassen sich nicht mehr blind auf Videomeeting und wollen dann auch ein amtliches Lichtbilddokument zur Verifizierung sehen. Es ist hier mehr als erschreckend, dass man in diesem Zusammenhang im Darknet wirklich alles kaufen kann, auch „amtliche Ausweisdokumente".

Nachfolgend einmal eine aktuelle Preisliste, was so etwas im Darknet kosten würde:

Ausweis mit folgenden Charakteristika:
- Mikro-Schriftzug (600 dpi)
- Wassermarke und Siegel
- Hologramm
- integriertes Hintergrundmuster
- maschinenlesbare Zone

Preis: 250 – 350 Euro

Führerschein:
Preis: 250 – 350 Euro

Reisepass:
Preis: 1.000 Euro

Natürlich wird in diesem Artikel nicht die Adresse veröffentlicht, wo man diese Artikel kaufen kann.

Aber es ist erschreckend, dass man so etwas so günstig kaufen kann, zumal mit derartigen Dokumenten so viele kriminellen Taten mit schwerwiegenden Folgen realisiert werden können.

Dass Europol und andere Polizeibehörden nicht hiergegen einschreiten ist ebenfalls nicht nachvollziehbar.

Theoretisch könnte man natürlich sagen: Woher will denn der Cyberkriminelle bzw. der Cyberterrorist wissen, dass XYZ für die Cybersecurity beim Betreiber der Kritischen Infrastruktur ABC zuständig ist.

Das Internet vergisst nie etwas

Bereits vor 21 Jahren, d.h. im November 2001 wurde das NATO Open Source Intelligence Handbook veröffentlicht und bis heute kann es als Grundlagenwerk angesehen werden [18]. Schauen wir uns an, wie Cyberkriminelle, aber auch Geheimdienste auf legale Informationen an alle Informationen über uns kommen.

Alles beginnt damit, dass man sich eine Person aussucht, die in der Hierarchie im Unternehmen oben steht, aber von den meisten nicht persönlich gekannt wird, zugleich aber eine entsprechende Macht im Unternehmen hat, so dass man ihr in der Regel nicht widersprechen sollte (z.B. Leiter IT, Geschäftsführung, Leiter Personalabteilung). Über google kann hier problemlos über die Schlagwörter Unternehmen, Organigramm der Aufbau des Unternehmens gefunden werden. Wenn man Glück hat, findet man dann auch gleich Name, Foto und Lebenslauf dieses Entscheiders.

Die Suche nach privaten und dienstlichen E-Mail-Adressen sowie privaten und dienstlichen Festnetz- und Mobilfunknummern der entsprechenden Personen erhält man dann über entsprechende Suchdienste (i.d.R. in den USA angesiedelt):

Rocket Research [19]
Lusha [20]
Hunter [21]

In der Regel finden sich hierüber wichtige Kommunikationsdaten über die entsprechenden Personen. Die Mobilfunknummer des britischen Premierministers Boris Johnson war zum Beispiel über Jahre hinweg leicht zu finden.

Oftmals finden sich in Sozialen Netzen ebenfalls Informationen über:
- Geburtsdatum
- Persönliche Interessen
- Freunde, Bekannte
- Netzwerke
- Politische Einstellung

etc.

Relevante Netzwerke sind hierbei:
- Facebook
- LinkedIn
- Twitter
- Instagram
- Telegram

Will man dann wissen, wo sich jemand aufhält (natürlich nur beim Mobilfunk relevant), so gibt es Tools (im normalen Internet), mit den man Cell-Tracking auf einfachste Art und Weise betreiben kann [22]. Auch bei ausgeschalteten Handys erfährt man problemlos:

Ist die Telefonnummer noch gültig?

Ist die Telefonnummer an das Netz angeschlossen, z.B. Vodafone UK

Ist der Benutzer im Roaming-Modus

Wird die Nummer portiert

Will man dann noch die Adresse erfahren, so bedarf es weiterer Tools im Darknet. Da dies nicht legal ist, werden hierzu keinerlei Angaben gemacht.

Nun wissen CISOs und CIOs natürlich, dass Kriminelle – die keine E-Mail-Adresse von einer entsprechenden Führungskraft gefunden haben – hier den allgemeinen Algorithmus nutzen, wie E-Mail-Adressen aufgebaut sind, zum Beispiel: aaa.bbb@gold-energy.com. Sendet der Angreifer dann eine E-Mail an diese Adresse täuschen gute CISOs die Nicht-Erreichbarkeit zum Beispiel durch die folgende Meldung vor: „Ihre Nachricht an aaa.bbb@gold-energy.com wurde blockiert“ Es wird dann noch ausgegeben: 550.5.4.1 Recipient address rejected: Access denied. Trotzdem wurde die Adresse zugestellt. Nun gibt es Programme, die umgehend ein Feedback geben, wann diese Nachricht jeweils gelesen wurde. Selbst in IT-technisch sehr versierten Ländern wie China hat man derzeit kaum eine Chance, dies zu blocken. Diese Programme sind im Internet frei verfügbar. Trotzdem werden diese hier nicht genannt.

Bevor wir nachfolgend zu dem wichtigen Tool maltego kommen, sei an dieser Stelle noch kurz auf die Bild-Tools verwiesen, welche Cyberkriminelle nutzen.

Das in Bild 5 gezeigte Bild wurde übersandt, um einem Leiter IT zu belegen, dass gerade XYZ verunglückt sei und man deshalb Zugang zu 123 benötigt. Eine gute Masche von Kriminellen, wobei dies jedoch deshalb in diesem Falle innerhalb von 4 Stunden auffiel, weil dieses Bild bereits durch einfache google-Bildrecherche als zwei Jahre altes Unfall-Bild erkannt wurde, welches hundertfach im Netz finden ist. Zur Standardabwehr der Gefahrenabwehr sollte stets jedes Bild, welches von Dritten übersandt wird, auf Echtheit verifiziert werden [23]

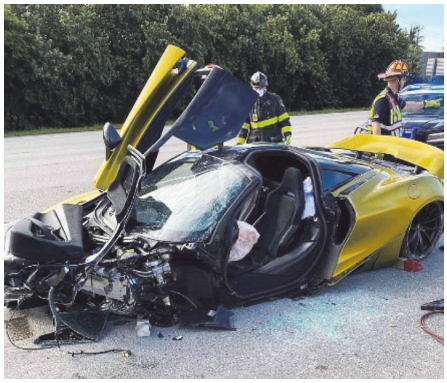


Bild 5. Autounfall in London Quelle: youtube, tiktok u.a.

Im besagten Falle wurde dann auch noch kommuniziert, dass man die nächsten Tage auch nicht dem verunglückten XYZ kommunizieren könne, da er im Koma sei und in die USA verbracht worden sei. In diesem Falle konnte aber einfachst verifiziert werden, dass das Mobilfunktelefon sich hiernach nie im Roaming Modus befand.

Dies mag belegen, dass manche Cyberkriminelle ihr Handwerk nicht immer hinreichend beherrschen.

OSINT Recherche über Kali-Linux

Wir haben bereits auf OSINT verwiesen. Aber was ist OSINT? Open Source Intelligent Tools ist gemäß der [übersetzten] Definition des US-amerikanischen Department of Defense (DoD) wie folgt definiert: „erstellt aus öffentlich verfügbaren Informationen, die gesammelt, ausgewertet und kurzfristig unter geeigneten Adressaten verbreitet werden, um besondere nachrichtendienstliche Anforderungen zu erfüllen“.

Die Vorgehensweise bei OSINT ist dabei relativ einfach:
- Öffentliche Assets aufspüren
- Relevante Informationen außerhalb der Organisation finden
- Ermittelte Informationen verwertbar zusammenstellen.

Eine sowohl für Hacker als auch für Cybersecurity-Fachkräfte wichtige Software ist zweifelsfrei Kali-Linux. Es handelt sich dabei um eine auf Debian basierende Linux-Distribution, welche vor allem Programme für Penetrationstests und digitale Forensik umfasst. Da Kali die GNU-GPL-Lizenz besitzt gilt Kali als Open Source.

Wichtige Kali-Linux Werkzeuge sind:
- Maltego:
  Programm, um Daten über Einzelpersonen oder Unternehmen im Internet zu sammeln
- Kismet:
  Passiver Sniffer zur Untersuchung von WLANS
- Social-Engineer Toolkit (SET):
  Programme für Penetrationstest mit dem Schwerpunkt auf Social Engineering
- Nmap:
  Netzwerkscanner zur groben Analyse von Netzwerken mit Zenmap
- Wireshark:
  Graphischer Netzwerksniffer
- Ettercap:
  Netzwerkadministrationstool (zum Beispiel für Man-in-the-Middle-Angriff)
- John the Ripper:
  Programm zum Knacken und Testen von Passwörtern
- Metasploit:
  Framework für das Austesten und Entwickeln von Exploits
- Aircrack-ng:
  Sammlung von Tools, die es ermöglichen, Schwachstellen in WLANs zu analysieren und auszunutzen
- Nemesis:
  Paketfälscher für Netzwerke
- RainbowCrack
  Cracker für LAN-Manager-Hashes
- The Sleuth Kit
  Sammlung von Forensik-Werkzeugen

An dieser Stelle sei ausdrücklich erwähnt, dass der Besitz von Kali Linux nicht strafbar ist, obgleich dies gerne so kommuniziert wird.

Um alle [verfügbaren] Informationen über Personen zu finden, ist eine Analyse – Software wie maltego [24] immer der richtige Anfang. Hier findet man immer etwas. Mit diesem Data-Mining-Werkzeug werden Informationen im Internet gesucht und verknüpft und die gefundenen Informationen werden mittels gerichteter Graphen dargestellt und lassen weitere Analysen zu. Die hierzu benutzten Quellen der Informationssuche sind Webseiten, soziale Netzwerke, Suchmaschinen oder öffentlich verfügbare Datenbanken.

Mittlerweile werden OSINT Tools theoretisch der breiten Öffentlichkeit vorgestellt [25]. Nach wie vor werden diese Fachartikel aber eher von Cyberkriminiellen denn von der Gegenseite gelesen.

Mit shodan.io wird es interessiert

Shodan sammelt Daten meist auf Webservern (HTTP/HTTPS über die Ports 80, 8080, 443, 8443), sowie FTP (Port 21), SSH (Port 22), Telnet (Port 23), SNMP (Port 161), SIP (Port 5060), und Real Time Streaming Protocol (RTSP, Port 554).

Eingesetzt wird shodan.io zur Gefahrenabwehr bei Betreibern kritischer Infrastrukturen wie der Energiewirtschaft, Wasser/Abwasserwirtschaft aber auch dem Bank- und Börsenwesen. Im umgekehrten Falle wird shodan.io aber auch zum Auffinden von Schwachstellen verwandt. Hierzu gibt es auch einen sehr aktuellen Fall, der allerdings nur anonymisiert wiedergegeben werden kann:

Die Organisationen A und B hatten offiziell nichts miteinander zu tun. Cyberkriminelle erkannten jedoch, dass die Organisationen enger verbunden sind als nach außen kommuniziert wurde.

Bei A konnten über shodan.io konnten sieben verwundbare Systeme (England, Indien, USA, Österreich, Spanien, Niederlande) verifiziert werden; bei B konnten über shodan.io vier verwundbare Systeme (Indien, USA, Niederlande). Bei den Systemen von B konnte die gleiche IP-Adresse gefunden werden wie bei A. Eine geeignete Schwachstelle fand man über die cloud Systeme und die Virtuelle Maschinen. Somit konnte man über das eine Systeme unbemerkt auf die Systeme der anderen Organisation zugreifen.

Das sogenannte „Abziehen“ verwertbarer Daten dauerte dann vier Tage. Es handelt sich hierbei um große und bedeutende Organisationen, bei denen man eigentlich größere Cybersecurity hätte erwarten können. Aber vielleicht sind Cyberkriminelle ja in einer der Organisationen von A und B fix installiert.

Auch wenn hier sicherlich viele an Details interessiert sein sollten, so dürfen aus rechtlichen Gründen keinerlei weiteren Auskünfte gegeben werden können.

Vorausgegangen – quasi zur Qualitätskontrolle – war eine Art Stealth Scanning. Eine Version sei hier vorgestellt:

Nach wie vor achten die meisten Firewalls auf SYN Pakete, FIN Pakete können unbemerkt durchschlüpfen. Es wird also ein Port Scan mit einem Paket und dem FIN Flag übersandt. Es wird keine Antwort erwartet. Erhält man eine RST Rückmeldung, kann man davon ausgehen, dass der PORT geschlossen ist. Wenn man nichts erhält, deutet dies darauf hin, dass der Port offen ist.

Beim X-Mas Scan wird ein Paket gesetzt, bei dem die Flags FIN, URG und PUSH gesetzt sind. Dabei wird entweder eine RST-Rückmeldung oder gar keine Rückmeldung verlangt.

Gerade bei Nicht-Windows-Systemen kommt man bei den Weiterentwicklungen der vorstehend beschriebenen Stealth Scannings an fast jeder Firewall vorbei.

Fazit

Es ist heutzutage kaum mehr möglich zu wissen, ob man wirklich in einem Online-Meeting mit der Person ist, mit der man glaubt in einem Meeting zu sein. Und es wird auch immer einfacher sich die entsprechende Hardware zu besorgen, wenn man zum Beispiel nicht die benötigte NVIDIA Karte oder nur eine langsame CPU hat. In einem solchen Fall nutzt man nämlich einfach Googles Lab.

Natürlich kann man jetzt entgegnen, dass es doch Programme gibt, die aufzeigen können, ob ein digitales Erzeugnis ein Fake ist. Hier ist zum Beispiel Amped Authetic zu nennen. Hat man Zeit, so ist dies kein Problem. In Krisensituationen wird man diese Zeit jedoch in der Regel nicht haben. Dann bliebt oftmals nichts anderes übrig, als sich auf den „gesunden Menschenverstand“ zu verlassen.

Celltracker, E-Mail-Tracker sind Gefahrenquellen, die immer noch nicht hinreichend bekannt und abgewehrt werden. Dies gilt auch für entsprechende OSINT Werkzeuge sei es das KALI Linux Tool maltego oder das mächtige shodan.io oder das „Stealth Scanning.“ Hier besteht ein großer Trainingsbedarf bei den entsprechenden Fachkräften für Cybersicherheit. Noch ist der Krieg nicht verloren, denn oftmals machen die meisten Cyberkriminellen die gleichen Fehler wie angegriffenen Institutionen, so dass man relativ einfach verifizieren kann, wer die bösen Menschen sind.

Quellen

[1] https://versicherungsmonitor.de/2019/06 /21/neue-sprachmasche-bei-fake-president/

[2] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

[3] https://www.deutschlandfunk.de/kuenstliche-intelligenz-lyrebird-ein-leierschwanz-fuer-jede-100.html

[4] https://events.vgbe.energy/events/keli-2022/6693/JG3UR/program/talk/wie-cyberkriminelle-die-identitaet-einer-fuehrungskraft-eines-unternehmens-der-kritischen-infrastruktur-annehmen-und-was-man-gegen-social-engineering-tun-kann/65967/infos

[5] Christopher M. Bishop, Neural Networks and Machine Learning (NATO ASI Subseries F:, Band 168, Springer, ISBN-13: 978-3540649281.

[6] Ian Goodfellow, Yoshua Bengio, Aaron Courville: Deep Learning (= Adaptive Computation and Machine Learning). MIT Press, 2016, ISBN 978-0-262-03561-3.

[7] https://cs231n.github.io/convolutional-networks/

[8] https://www.pressetext.com/news/20180125022

[9] https://www.youtube.com/watch?v=s1D Phc9HNQ0

[10] https://proceedings.neurips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf

[11] Zhaohe Zhang, Qingzhong Liu: Detect Video Forgery by Performing Transfer Learning on Deep Neural Network. In: Advances in Natural Computation, Fuzzy Systems and Knowledge Discovery (= Advances in Intelligent Systems and Computing). Springer International Publishing, Cham 2020, ISBN 978-3-03032591-6, S. 415–422.

[12] https://proceedings.neurips.cc/paper/2019/fle/31c0b36aef265d9221af80872ceb62f9 -Paper.pdf

[13] https://proceedings.neurips.cc/paper/2019

[14] https://www.nzz.ch/digital/adobe-project-voco-photoshop-fuer-die-stimme-ld.126328

[15] http://research.baidu.com/Blog/index-view ?id=91

[16] https://arxiv.org/pdf/2112.02418v3.pdf

[17] E. Cooper, C.-I. Lai, Y. Yasuda, F. Fang, X. Wang, N. Chen, and J. Yamagishi, “Zero-shot multi-speaker text-to-speech with-state of the art neural speaker embeddings,” in ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP). IEEE, 2020, pp. 6184–6188.

[18] https://archive.org/details/NATOOSINTHandbookV1.2

[19] rocketreach.co

[20] lusha.com

[21] hunter.io

[22] https://www.cell-track.de/

[23] https://images.google.de

[24] https://kali.org/tools/maltego

[25] Computerwoche 15.06.2022: Die besten OSINT Tools.

[26] https://ieeexplore.ieee.org/abstract/document /8954668 (The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends).

[27] https://link.springer.com/chapter/10.1007/978-1-4842-3838-7_10 (Gathering Evidence from OSINT Sources).

vgbe Fachtagung

Brennstoffe, Feuerungen und Abgasreinigung 2022

28. und 29. September 2022
in Hamburg | Hotel Gastwerk mit Fachausstellung

Brennstoffe, Feuerungen und Abgasreinigung 2022

Mit der Fachtagung „Brennstoffe, Feuerungen und Abgasreinigung 2022“ am 28. und 29. September 2022 im Hotel Gastwerk in Hamburg starten wir in diesem Jahr ein neues Format, das die wesentlichen Aspekte und Auswirkungen des Einsatzes unterschiedlicher Brennstoffe auf die Feuerung und Abgasreinigung berücksichtigt.

Kohle war die treibende Kraft hinter der industriellen Revolution und veränderte den Kurs der ganzen Welt. Heute befinden wir uns wieder in einem dramatischen Kurswechsel und ersetzen Kohle durch alternative Brennstoffe oder alternative Stromerzeugungsverfahren. In dieser Übergangsphase ist es wichtig, sowohl der auslaufenden Kohlenutzung weiterhin eine Plattform zu bieten, als auch die integrale Auswirkung alternativer Brennstoffe oder Verfahren zu betrachten.

Die Fachtagung „Brennstoffe, Feuerungen und Abgasreinigung 2022“ bietet Betreibern, Herstellern, Planern, Genehmigungsbehörden und Forschungsinstituten eine Plattform die aktuellen Herausforderungen der Energiepolitik zu diskutieren.

Wir freuen uns auf ihre Teilnahme an der vgbe-Fachtagung im September in Hamburg.

In die Veranstaltung ist eine begleitende Fachausstellung integriert, die zusätzliche Informationsmöglichkeiten bietet.

Auf Wiedersehen in Hamburg!

Ihr vgbe-Team

Tagungsprogramm

Änderungen vorbehalten

MITTWOCH, 28. SEPTEMBER 2022

ab 18:00	*Get-Together im Hotel*

DONNERSTAG, 29. SEPTEMBER 2022

ab 08:00	*Registrierung und Welcome-Kaffee*
08:30-08:40	Begrüßung
08:40 – 09:00 V1	Zukunft der konventionellen Kraftwerke aus Sicht des vgbe energy *Dr. Thomas Eck, vgbe energy, Essen*
09:00 – 09:30 V2	Lagerschäden an Schüsselmühlen – Ergebnisse der Schadensanalyse und daraus abgeleitete Condition Monitoring Maßnahmen *Dr. Gereon Lüdenbach, Patrick Gehlmann, StandZeit GmbH, Coesfeld, Martin Fricke, Trianel, Lünen*
09:30 – 10:00 V3	Möglichkeiten der messtechnischen Bestimmung des Betriebsverhaltens von Mahlanlagen einschließlich der Brenner und Feuerung als Basis für Bewertungen und Optimierungen *Dr. Steffen Griebe, Dipl.-Ing. Helge Kaß, Dipl.-Ing. Volker Biesold, Dipl.-Ing. (FH) Peter Lange, Dipl.-Ing. (FH) Rene Wascher, M. A. Adrian Weber, VPC, Vetschau/Spreewald*
10:00 – 10:30 V4	Online-Korrosionsmonitoring in Kraftwerksfeuerungen *Prof. Dr. B. Epple, A. Marx, D. Hülsbruch, Technische Universität Darmstadt, Institute for Energy Systems & Technology (EST)*
10:30 – 11:00	*Kaffeepause in der Ausstellung*
11:00 – 11:30 V5	Einsatz von längsnahtgeschweißten Alloy-Rohren in Überhitzerbündeln und Membranwänden *Dipl.-Ing. Uwe Schadow, Steinmüller Engineering GmbH, Gummersbach*
11:30 – 12:00 V6	Ammoniak als alternativer Brennstoff *Dr. Anne Giese, Gas-Wärme-Institut e.V., Essen*

Online-Anmeldung

https://register.vgbe.energy/21622/

Kontakt (Teilnahme)

Barbara Bochynski | t +49 201 8128-205 |
e vgbe-brennstoffe@vgbe.energy

12:00 – 12:30 V7	GKM und die Energiewende *Peter Volkmann,* *Leiter Betrieb GKM, Mannheim*
12:30 – 13:30	*Lunch*
13:30 – 14:00 V8	Multifuel Feuerung in der zirkulierenden Wirbelschicht *Frank Leuschke,* *Doosan Lentjes GmbH, Ratingen*
14:00 – 14:30 V9	Effiziente Analyse und Bewertung des Verbrennungsprozesses durch Ermittlung relevanter Prozessgrößen *Ismail Korkmaz,* *EUtech Scientific Engineering, Aachen*
14:30 – 15:00 V10	Innovative Vergasungstechnologien für das chemische Recycling von Reststoffen *E. Langner, Prof. Dr. B. Epple, J. Ströhle,* *Technische Universität Darmstadt,* *Institute for Energy Systems & Technology (EST)*
15:00 – 15:20	*Kaffeepause in der Ausstellung*
15:20 – 15:50 V11	REA-Ertüchtigung im Kraftwerk Lippendorf *Dr. Dorian Rasche,* *Steinmüller Eng., Gummersbach;* *G. Heinze,* *Lausitz Energie Kraftwerke AG, Cottbus*
15:50 – 16:20 V12	Verfahren der Hg-Minderung – Ein Überblick zu gängigen Maßnahmen *Jan Schütze,* *IEM FörderTechnik GmbH, Kastl*
16:20 – 16:50 V13	Investigations on the separation potential of different dust removal systems for automatically-fed biomass boilers *M.Sc. Javier Carrillo, M.Sc. Marc Oliver Schmid,* *Dr.-Ing. Ulrich Vogt,* *IFK, Universität Stuttgart*
16:50 – 17:00	Schlusswort Ende der Fachtagung

Organisatorische Hinweise

VERANSTALTUNGSWEBSEITE

w https://t1p.de/vgbe-bfa2022 (Kurzlink)

VERANSTALTUNGSORT

Gastwerk Hotel Hamburg
Beim Alten Gaswerk 3
22761 Hamburg
t +49 40 89062-498
e reservation@gastwerk-hotel.de
w www.gastwerk.com

ONLINE-ANMELDUNG

w https://register.vgbe.energy/21622/

ANMELDUNG

Die Anmeldung wird bis zum 19. September 2022 erbeten (Redaktionsschluss der namentlichen Nennung im Teilnahmeverzeichnis). Eine spätere Anmeldung, auch im Tagungsbüro, ist möglich, jedoch ohne Aufnahme in das Teilnahmeverzeichnis.

TEILNAHMEBEDINGUNGEN

vgbe-Mitglieder	620,- €
Nichtmitglieder	780,- €
Hochschulen, Behörden, Ruheständler	300,- €
Studierende	frei mit Nachweis

FACHAUSSTELLUNG

Um Ihre Dienstleistungen und Produkte in den Fokus zu rücken, bieten wir Ihnen auf der Fachtagung die Gelegenheit zur Firmenpräsentation:
| Paket P (inkl. 1 Konferenzticket) für
€ 920 + USt. (vgbe-Mitglieder*)
€ 1.080 + USt. (Nicht-Mitglieder),
Kontakt:
Steffanie Fidorra-Fränz
t +49 201 8128-299
e steffanie.fidorra-fraenz@vgbe.energy

** Gerne Informieren wir Sie auch über Konditionen und Leistungen einer vgbe-Mitgliedschaft.*

vgbe energy e.V.

Deilbachtal 173
45257 Essen

be informed

www.vgbe.energy

ENERGY IS US