



14. TTZ-WUE Projekt, das Informationen über Cyberangriffe sammelt, bevor diese Schlagzeilen machen

Prof. Dr. Sebastian Biedermann

Das Technologiezentrum Würzburg zum Thema Cyber-Sicherheit

Das **TTZ-WUE** beschäftigt sich mit den realen Herausforderungen moderner Cyber-Sicherheit. Im Fokus stehen nicht abstrakte Modelle, sondern konkrete Angriffe, reale Infrastrukturen und verwertbare Erkenntnisse für Wirtschaft, Verwaltung und Gesellschaft. Das Institut verbindet angewandte Forschung

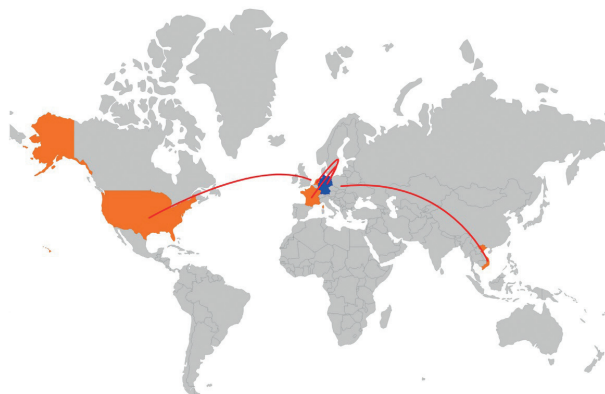
mit Lehre und Technologietransfer und arbeitet eng mit regionalen wie überregionalen Partnern zusammen.

Neben zahlreichen anderen Themen der Cyber-Sicherheit liegt ein besonderer Schwerpunkt auf der Analyse aktueller Bedrohungen im Cyberraum und deren frühzeitiger Erkennung. Dazu hat das Institut eigene Forschungsinfrastrukturen, die kontinuierlich unter realen Bedingungen betrieben werden. Studierende werden aktiv in Projekte eingebunden und arbeiten mit echten Daten statt synthetischer Beispiele.

Quellländer von digitalen Angriffen (links) und Live-Angriffe visualisiert auf einer Weltkarte.

last 3 days

	Value	Count	Info
1	Romania	408946	 Romania
2	United States	196953	 United States
3	The Netherlands	82941	 The Netherlands
4	France	56261	 France
5	Brazil	33420	 Brazil
6	Vietnam	24173	 Vietnam
7	United Kingdom	23684	 United Kingdom
8	China	22657	 China
9	Bulgaria	18050	 Bulgaria
10	Russia	13429	 Russia



Quelle: TTZ-WUE Honeynet

Ziel ist es, Cyber-Sicherheit nicht nur reaktiv zu denken, sondern vorausschauend und datengetrieben. Die gewonnenen Erkenntnisse fließen sowohl in Forschungsprojekte als auch in Lehrveranstaltungen, Abschlussarbeiten und Transferformate ein. So entsteht ein Kreislauf aus Beobachtung, Analyse und Anwendung, mit dem Anspruch, digitale Sicherheit messbar und verständlich zu machen.

Ein Messinstrument für digitale Bedrohungen

Es sieht unscheinbar aus, hat kein schweres Stahlgehäuse und kein dramatisches Warnsignal, lediglich ein Dashboard blinkt hin und wieder auf. Und doch ist es eines der sensibelsten Messinstrumente unserer digitalen Gegenwart: Das TTZ-WUE Honeynet, verteilt über ganz Deutschland, ständig online, ständig angegriffen. Die Aufgabe dieses Systems ist angegriffen zu werden. Über 5.000 Events werden pro Stunde gesammelt. Automatisierte Scans, Exploits, Brute-Force-Versuche und neuartige Angriffsmuster prallen auf unsere verteilten Systeme.

Was hier landet, landet manchmal erst Tage oder Wochen später in realen Unternehmensnetzen. Das TTZ-WUE Honeynet ist ein Art Frühwarnradar für digitale Angriffe.

Wenn Angreifer willkommen sind

Ein Honeypot ist ein bewusst verwundbares IT-System, das Angreifer anzieht. Anders als klassische Sicherheitssysteme versucht es nicht, Angriffe zu verhindern, sondern diese sichtbar zu machen. Ein Honeynet geht einen Schritt weiter: Es besteht aus vielen verteilten Honeypots. Im Projekt kommen High-Interaction Honeypots zum Einsatz. Das bedeutet, die Angreifer interagieren nicht mit Attrappen, sondern mit echten Betriebssystemen, echten Diensten, echten Konfigurationsfehlern. Jeder Login-Versuch, jeder eingegebene Befehl, jedes nachgeladene Schadprogramm wird detailliert aufgezeichnet und analysiert.

Unsere Honeypots sind ausschließlich in Deutschland platziert. Damit lassen sich Angriffe gezielt auf regionale Besonderheiten, Branchenfokus oder neue Kampagnen analysieren.

Unauffällig, aber verlockend

Das Honeynet des TTZ-WUE besteht aus einer verteilten Server- und VM-Infrastruktur, die verschiedene Zielsysteme abbildet: Linux- und Windows-Server, Typische Unternehmensdienste (SSH, RDP, Web-Anwendungen, Datenbanken, u.v.m.), unterschiedliche Patch- und Konfigurationsstände.

Eingehende Events von verschiedenen IP-Adressen, z. B. Login-Versuche

time	source	country	event
2026-04-21 13:26:32	148.135.x.x	 United States	failed login (SSH) with username '09c59293b7751c6ce8ede81d258a00dc' and password '961d3fde2705ba0f0d6af975b8877847'
2026-04-21 13:26:32	23.94.x.x	 United States	failed login (SSH) with username 'd67d53494e0ed6fad778ba49ae695a38' and password '60c2b2b6e97b02fc77310da89390734c'
2026-04-21 13:26:32	178.216.x.x	 Russia	connection attempt to TCP port 9001
2026-04-21 13:26:32	178.216.x.x	 Russia	connection attempt to TCP port 9001
2026-04-21 13:26:32	178.216.x.x	 Russia	connection attempt to TCP port 9001
2026-04-21 13:26:32	178.216.x.x	 Russia	connection attempt to TCP port 9001
2026-04-21 13:26:32	94.154.x.x	 The Netherlands	successful login (SSH) with username 'root' and password 'end123'
2026-04-21 13:26:32	178.216.x.x	 Russia	connection attempt to TCP port 9001
2026-04-21 13:26:29	103.187.x.x	 Indonesia	failed login (SSH) with username 'appserver' and password 'appserver'
2026-04-21 13:26:29	45.142.x.x	 Romania	connection attempt to TCP port 16297
2026-04-21 13:26:30	37.10.x.x	 United Kingdom	requested file on the Web server
2026-04-21 13:26:30	37.10.x.x	 United Kingdom	requested file on the Web server

Quelle: TTZ-WUE Honeynet

Ransomware Cyberangriff zeigt persönliche Dateien verschlüsselt



Die Hardware selbst ist bewusst unspektakulär: Standard-Server, Virtualisierung, abgesicherte Management-Netze. Der Fokus liegt nicht auf exotischer Technik, sondern auf Realismus. Genau das macht die Systeme für Angreifer attraktiv.

KI als Übersetzer feindlicher Aktionen

Durchschnittlich mehrere tausend Ereignisse pro Stunde lassen sich nicht mehr manuell auswerten. Klassische, regelbasierte Analyseverfahren stoßen hier ebenfalls schnell an ihre Grenze. Sie erkennen bekannte Muster zuverlässig, übersehen jedoch neue oder leicht abgewandelte Angriffstechniken. Um diese Lücke zu schließen, wurde das Honeynet um KI-gestützte Analyseverfahren erweitert, die nicht einzelne Events isoliert betrachten, sondern Zusammenhänge erkennen sollen und einen menschlichen Beobachter unterstützen.

Die eingesetzte KI-Software interpretiert digitale Angriffe dabei wie eine Sprache mit eigener Grammatik. Sie analysiert nicht nur, dass ein Angriff stattfindet, sondern wie er durchgeführt wird. So werden etwa Sequenzen von eingegebenen Shell-Befehlen ausgewertet: Ob ein Angreifer systematisch Informationen sammelt, gezielt nach Schwachstellen sucht oder versucht, sich dauerhaft im System festzusetzen, lässt sich häufig bereits aus wenigen Befehlen ableiten.

Auch hochgeladene Dateien werden automatisch untersucht. Die KI bewertet deren Struktur, Funktion und typische Nutzungsmuster, etwa ob es sich um einen Downloader, ein Backdoor-Programm oder ein Werkzeug zur lateralen Bewegung im Netzwerk handelt. Ergänzend dazu werden digitale Spuren wie

User-Agents, verwendete Protokolle oder charakteristische Befehlsfolgen mit bekannten Angriffswerkzeugen und Kampagnen abgeglichen.

Auf diese Weise entstehen aus vielen scheinbar isolierten Einzelereignissen zusammenhängende Angriffsbilder. Die KI hilft dabei, neue Angriffskampagnen frühzeitig zu erkennen, bekannte Muster einzuordnen und Abweichungen sichtbar zu machen, oft lange bevor entsprechende Techniken in realen Unternehmensnetzen oder öffentlichen Lageberichten auftauchen.

Ein Beispiel eines eingegebenen Befehls mit KI-Analyse aus dem Projektalltag:

Command of an attacker	Automated AI analysis
uname -s -v -n -m 2 > /dev/null	The command queries the system's kernel name, kernel version, network node hostname and hardware architecture. By discarding the output ('> /dev/null') the attacker is only interested in whether the command succeeds and can later use the exit status to confirm the target's OS type and architecture for tailoring an exploit. This information helps the malicious user decide which payload or attack vector will work on the compromised host.

Künstliche Intelligenz hilft dabei, neue Angriffskampagnen frühzeitig zu clustern, Anomalien zu erkennen und bekannte Muster von wirklich neuen Techniken zu trennen.

Cyber-Sicherheit als Frühwarnsystem

Aktuell dient das TTZ-WUE Honeynet als angewandte Forschungsplattform: Trends erkennen, Angriffswerkzeuge verstehen, Bedrohungen einordnen. Studierende finden hier Daten für Abschlussarbeiten und Projekte.

Der nächste Schritt ist deutlich ambitionierter, aber konsequent: Der Ausbau zu einer Cyber-Lagebildplattform. Ziel ist ein System, das aktuelle Angriffstrends visualisiert, Eskalationen früh automatisiert erkennt und Entscheidungsträgern ein verständliches Lagebild liefert.

Statt reiner Log-Daten entsteht ein dynamisches Bedrohungsbild: Was passiert gerade? Wie neu ist das? Wie relevant? Und für wen? Gerade für kleine und mittlere Unternehmen, Kommunen oder kritische Infrastrukturen kann ein solches Lagebild den Unterschied machen.

Short Facts:

Thema

Cyber-Sicherheit

Leitung

Prof. Dr. Sebastian Biedermann

(Spezial-)gebiete

**Malware Analyse
Schwachstellensuche
Threat Intelligence**

Standort & Kontakt

**Tückelhäuser Str. 10 / 1.OG
97199 Ochsenfurt
ttz-wue@thws.de**