SUCCESS STORY

CYBERTRAP: HACKER IN DIE FALLE LOCKEN

CYBERTRAP Software GmbH
Auerspergstraße 4/7, 1010 Wien
Tel. +43(0)1 890 47 00
office@cybertrap.com

Kleinunternehmen Wien
Förderung: Basisprogramm

Deception Technologie aus Österreich

FANGEN SIE HACKER IN EINER ÜBERWACHTEN UMGEBUNG EIN UND ANALYSIEREN SIE SIE

Cyberattacken werden immer komplexer und professioneller. Bei den meisten attackierten Organisationen handelt es sich um wiederkehrende Attacken derselben Angreifer, weshalb die Idee entstand, diese in eine intelligente Falle zu locken und sie glauben zu lassen, erfolgreich ins Ziel-System eingedrungen zu sein. Ziel ist die Entwicklung einer Plattform, die einem potentiellen Angreifer ein der tatsächlichen Unternehmensgröße entsprechendes Netzwerk vortäuscht und dadurch den Angriff von den reellen Ressourcen abhält sowie die Angriffsmethodik transparent macht.

Innovationsgehalt und Nutzen

Am europäischen Mark zählt das Cyber-Security Produkt von CYBERTRAP nach wie vor zu den technisch ausgereiftesten Lösungen. Die **extrem schnellen Veränderungen im Cyber-Security Umfeld** verlangen eine permanente Forschungsarbeit und Weiterentwicklung. Zurzeit sind **nur wenige Deception Produkte** am Markt verfügbar, **die die speziellen Anforderungen einer Cybertrap erfüllen** und mit dem verfolgten technischen Lösungsansatz einer simulierten Umgebung vorgeht. Die Entwicklung stellt eine Neuheit für den Markt dar.

- **Rasche Erkennung** von Hackerangriffen
- **Minimierung des Schadens** durch Hackerangriffe
- **Gewinnung von wertvollen Threat Intelligence Daten**

*Foto (von links oben nach unten): Das CYBERTRAP-Kernteam **arbeitet in Echtzeit**: Franz Weber, Gerald Wallner, Dominik Turner, Jakob Maier, Stefanie Scholz, Tobias Schlattmann, Yunus Tuncel und Maik Binjaminov*

Österreichische
Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at

SUCCESS STORY

Cyberattacken zunehmend komplexer und professioneller

Es ist eine Tatsache, dass Cyberattacken immer **komplexer und immer professioneller** werden. Dies ist einerseits dadurch getrieben, dass sich hinter den Attacken inzwischen **eine ganze „Industrie“** mit dem Ziel Informationen zu erhalten, welche dann auf **ungesetzliche Weise** weiterverwendet wird. Auf der anderen Seite gibt staatlich gelenkte Institutionen, die sich zwar **unter dem Mantel der Legalität bewegen** und das klare Ziel haben ebenfalls an Informationen zu kommen, welche zu deren strategischen Vorteil genutzt werden können oder gezielt Systeme stören wollen.

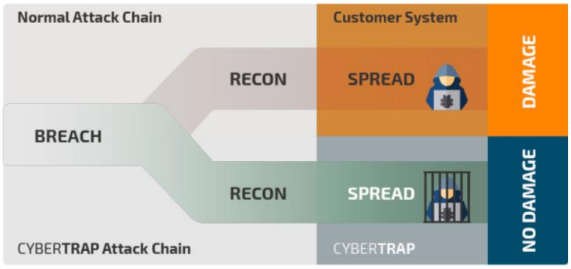
Weiters ist eine interessante Beobachtung, dass die **überwiegende Mehrheit der attackierten Organisationen mit wiederkehrenden Attacken derselben Angreifer zu tun** hatte, deshalb entstand die Idee, diese in eine **intelligente Falle (Cybertrap)** zu locken und sie in dem Glauben zu lassen, erfolgreich ins Ziel-System eingedrungen zu sein, um so einzigartige Information über die Angreifer zu erlangen.

Cyberattacken gezielt mit Forschungsstrategie begegnen

Die **Profession und das Know-how der Cybertrap sowie die Ziele eines Unternehmens** bedingen eine ständige Weiterentwicklung, welche auch durch die Schnelllebigkeit der IT-Branche bedingt ist.

Das Prinzip der Cybertrap-Falle ist es, eine horizontale Diversifikation (zusätzliche Angriffs-vektoren) in diesem Bereich anzustreben, denn hier ist ein sehr großes Potential gegeben. Vor allem im Endpoint und Tablet-Bereich, welcher bis dato nicht oder nur unzureichend geschützt wird, sieht man für derartige Sicherheitssysteme ein beträchtliches **Potential bzw. großen Nachholbedarf der Industrie** (Stichwort: Industrie 4.0, IT-Security).

Abbildung 1: Das Prinzip der Cybertrap-Falle



Weitere Bespiele dafür sind das **Absichern von Schulnetzwerken** (zB alle Gymnasien in einem Land usw.) und **öffentliche und halböffentliche Stelle**n (zB Spitäler, Behörden).

Die Deception-Technologie dahinter

Active Directory (AD) ist ein Standardwerkzeug, das von den meisten Organisationen verwendet wird, **um den Zugriff von Benutzern und Rechnern auf die Ressourcen des Unternehmens zu regeln**. Jeder Computer im Unternehmensnetzwerk muss daher einen gewissen Zugang zum AD haben, damit die Netzwerkumgebung korrekt funktioniert.

Angreifer setzen **Phishing, Man-in-the-Middle und andere Techniken** ein, um sich die Berechtigungen zu verschaffen, die sie benötigen, um in ein Netzwerk einzubrechen. Sobald sie einmal im System sind, setzen sie oft **Angriffswerkzeuge wie Bloodhound Scans** ein, um die gesamte AD-Umgebung abzubilden.

Durch diesen Abgleich können Angreifer die wertvollen Ressourcen, Systeme und privilegierten Benutzerkonten identifizieren, die sie zur **Erreichung ihrer Ziele und zur Erstellung eines Angriffsplans** benötigen. Durch den Zugang zum AD erhoffen sich Angreifer, sich **vor den Sicherheitsteams und ihren Werkzeugen zu verstecken**, indem sie zB vorhandene Zugangsdaten verwenden oder ihre eigenen Domains erstellen.

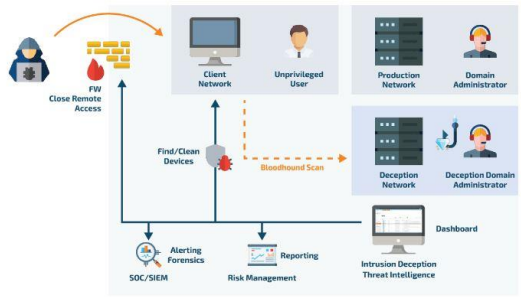
Österreichische
Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at

Wenn ein Angreifer **beispielsweise das Bloodhound-Tool verwendet, um AD nach „Admin-Konten“ zu scannen**, erhält er falsche Informationen zurück.

Damit geht sofort ein Alarm los und das Sicherheitsteam weiß, dass hier jemand unberechtigt nach „AD Admin-Konten“ sucht. **Nutzt der Angreifer die falschen Informationen**, um sich im Netzwerk weiter zu bewegen, wird er sofort wieder in eine sichere **Deception Umgebung umgeleitet**, wo er weiter beobachtet werden kann.

Während dies stattfindet **zeichnet CYBERTRAP die Techniken, Taktiken und Prozeduren der Angreifer auf**, die wiederum von einem operativen **Sicherheitsteam zur Stärkung der Abwehr im Produktivnetzwerk** eingesetzt werden, um weitere Angriffe zu verhindern.

Abbildung 2: Hacker werden systematisch in die Falle gelockt



CYPBERTRAP: Hersteller von Deception Technologie

Die CYBERTRAP Software GmbH wurde im Mai 2015 als Spin-off der SEC Consult Unternehmensberatung GmbH gegründet. Der Softwarehersteller mit Sitz in Wien ist seitdem rasch gewachsen und beschäftigt derzeit 15 Mitarbeiter*innen. Das Unternehmen ist europaweiter **Marktführer in puncto Deception-Technologie** und bietet seinen Kunden unkomplizierte Lösungen, die ihr Cybersicherheitsniveau nachhaltig verbessern.

Expansion in Europa

Die **von CYBERTRAP entwickelte Deception-Technologie** leitet Angreifer gezielt in eine eigens dafür geschaffene IT-Infrastruktur um, noch bevor sie weiter in die produktive Infrastruktur des Unternehmens eindringen können. Innerhalb dieser fiktiven Umgebung können sie systematisch beobachtet und ihre Motivation, Methoden und teilweise sogar ihre Identität und Auftraggeber identifiziert werden.

Das Potenzial dieser Technologie als ein Segment der **Wachstumsbranche Cybersecurity** ist durch die Digitalisierung enorm gestiegen. Denn die **durchschnittliche Verweildauer eines Angreifers in einem Netzwerk beträgt aktuell 56 Tage**, bevor die Attacke überhaupt erkannt wird. Und dann beginnt erst die forensische Arbeit, um den Angreifer aus dem System zu entfernen. Diese ressourcen- und kostenintensive Zeit kann **mit den CYBERTRAP-Lösungen jedoch um ganze 97 Prozent auf ein bis zwei Tage verringert werden**, was die massiven Folgekosten eines Angriffs signifikant reduziert.

Das Unternehmen hat in der D-A-CH-Region bereits ein **dichtes Partnernetzwerk etabliert und baut aktuell seine Position in Europa weiter aus**, beginnend in Spanien, Italien und den Benelux-Staaten. Vertriebspartnerschaften in zusätzlichen Märkten werden folgen. Die innovative Software wurde bei ihrer Gründung vor sechs Jahren unter anderem mit finanzieller Unterstützung der NÖ Bürgschaften und Beteiligungen GmbH, der Österreichischen Forschungsförderungsgesellschaft mbH und AWS – Austria Wirtschaftsservice zur Marktreife entwickelt. Die nunmehrige weitere Wachstumsfinanzierung ermöglicht CYBERTRAP die **Ausweitung dieser Expansionsstrategie**.

CYPERTRAP ist **zudem in Kooperation** mit dem Josef Ressel Labor TARGET, wo man über Sicherheitslösungen für zukünftige Bereiche Forschung und Entwicklung anstellt.

Österreichische
Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at