DATA SHEET CYBERSENSE DECEPTION

» EINBRUCHSERKENNUNG EINFACH UND **WIRKSAM**

CYBERSENSE Deception erkennt Einbrüche in Ihr Unternehmensnetzwerk oder Ihre Cloud-Umgebung einfach und wirksam. Cybersense Deception basiert auf einem komplementären Ansatz, der unabhängig von vorhandenen Sicherheitssystemen funktioniert. Während seiner Erkundungsphase greift der Angreifer auf präparierte Informationen zu, deren Nutzung sofortigen Alarm auslösen. Der Angreifer hat keine Chance zu erkennen, ob sein Lagebild real ist oder auf von Cybersense Deception vorgetäuschten Informationen beruht.

68% aller Einbrüche werden erst nach Wochen oder Monaten entdeckt.
(Quelle: Verizon, Data Breach Investigations Report 2018, Seite 6)

176 Tage dauert es in Europa durchschnittlich, bis ein Einbruch entdeckt wird.
(Quelle: FireEye Mandiant, M-Trends Report 2019, Seite 6)

» Die meisten Einbrüche basieren nicht auf den berüchtigten, hochkomplexen Angriffen. Vielmehr stehen dem Angreifer alle digitalen, sozialen oder physischen Methoden zur Verfügung, um sich einen ersten Eintrittspunkt zu verschaffen. Hier ist der Angreifer klar im Vorteil. Hat er erst einmal Zugang bekommen – meist mit geringen Nutzerrechten – versucht er, unter Nutzung einschlägiger Angriffstools, seine Befugnisse im Unternehmensnetz zu erweitern und seine Spuren zu verwischen.

» Hier ist die Schwachstelle des Angreifers, die sich Cybersense Deception zunutze macht. Der Angreifer befindet sich in einem ihm unbekannten Netzwerk und muss diese Umgebung zuerst erkunden. Zwar wird der Angreifer sehr vorsichtig vorgehen, aber letztlich muss er die erbeuteten Informationen nutzen, um mehr Informationen und erweiterte Rechte zu bekommen. Cybersense Deception infiltriert diesen Erkundungsprozess und bietet vorgetäuschte Informationen, die sofortigen Alarm auslösen.

» CYBERSENSE – **VORTEILE IM ÜBERBLICK**

- **» FRÜHZEITIGE ERKENNUNG**
  Alarmierung in der Erkundungsphase des Angreifers
- **» AGENTENLOS**
  Keine zusätzliche Software auf Clients oder Servern
- **» KOMPLEMENTÄR**
  Unabhängig von der vorhandenen Sicherheitsinfrastruktur
- **» BETRIEBSSICHER**
  Stört vorhandene IT nicht, ideal auch in KRITIS-Umgebungen wie Krankenhäusern
- **» KOSTENKONTROLLE**
  Einsetzbar auch in Teilbereichen des Unternehmensnetzes
- **» KEINE FEHLALARME**
  Nur die absichtliche Nutzung von Breadcrumbs löst Alarm aus

» ÜBER **CYBERSENSE**

Unsere Mission ist der Schutz von Unternehmensnetzwerken und sensibler Daten. Cybersense beginnt, wo konventionelle Sicherheitsmaßnahmen an ihre Grenzen stoßen. Unsere Technologie nutzt proaktiv die Schwächen von Angreifern und erkennt Einbrüche einfach und wirksam bevor Schaden entsteht.
Cybersense baut als Tochterunternehmen der concentrade auf die Expertise und Erfahrung von mehr als 20 Jahren im Bereich Cybersecurity auf.

DATA SHEET TECHNICAL FACTS

» CYBERSENSE DECEPTION **TECHNOLOGY**

Statt aus der Defensive zu agieren, geht Cybersense Deception offensiv vor: Im Unternehmensnetzwerk werden Breadcrumbs strategisch verteilt; auch in cloudbasierten Infrastrukturen und bei Einsatz von Cloud-Services. Die für den Angreifer vermeintlich interessanten Informationen verweisen auf Decoys und sind nicht von echten Anmeldeinformationen zu unterscheiden. Bei Interaktion mit einem Decoy wird sofort Alarm ausgelöst. Fehlalarme und Alarmmüdigkeit aufgrund vieler und bedeutungsloser Alarme sind damit ausgeschlossen. Gegenmaßnahmen werden unverzüglich eingeleitet, der Angreifer isoliert. Die Verweildauer des Angreifers wird auf ein Minimum reduziert und der Schaden minimiert.

» DEFINITIONEN

BREADCRUMBS werden umfangreich und strategisch im Netzwerk verteilt. Es handelt sich um Falschinformationen wie Registry-Einträge, Tokens oder Zugangsdaten. Sie locken Angreifer zu den Decoys.
DECOYS stellen sich dem Angreifer als Workstations oder Server dar. Für den normalen Anwender sind sie unsichtbar. Findet eine Interaktion mit einem Decoy statt, wird sofort ein Alarm ausgelöst.
MANAGEMENT Führt Analysen durch und überwacht.

» TECHNISCHE **DETAILS**

» BREADCRUMBS

- Vorwärtsverteidigung an den möglichen Eintrittspunkten
- dynamisch erzeugt
- automatisiert verteilt
- hohe Relevanz gegen Ransomware
- wirksam gegen APTs und Insider
- Manipulation der Ergebnisse gängiger Angriffswerkzeuge wie Mimikatz, BloodHound, GhostPack, Empire, Responder, ...
- Kundenspezifische Entwicklung möglich

» DECOYS

- Typischerweise VMs
- Kundenindividuell auf Maß erzeugt und individuell angepasst
- Verschiedenste Betriebssysteme

» MANAGEMENT

- Virtual Appliance
- On-Premise oder Cloud

» CYBERSENSE MANAGED SERVICE

- Unterstützung bei der Analyse von Alarmen
- Gewährleistung des kontinuierlichen Schutzes

»CYBERSENSE
Cybersense GmbH
Martin-Schmeißer-Weg 18 // 44227 Dortmund
Fon: +49 231 292974 00 // Mail: info@cybersense.de // **cybersense.de**