SAFELY ENABLING BUSINESS

Datasheet

Compromise Assessment

SecureLink unterstützt Ihre Organisation bei der Erkennung, Analyse und Beseitigung vorhandener Infiltrationen und kompromittierter Systeme sowie deren künftige Vermeidung.

Sie kommen leise...

... und sind geduldig. Sie gehen systematisch vor und versuchen so wenig Spuren wie möglich zu hinterlassen. Sie beobachten typische Routinen und imitieren diese, um unentdeckt zu bleiben. Sie entwickeln professionelle Angriffstools und -taktiken. Wochenlanges Totstellen ist ihnen ein Leichtes. Sie kommen wieder, wenn es sich lohnt. Sie handeln im Auftrag krimineller Syndikate und staatlicher Stellen. Es sind viele. Sie haben Ihre Organisation im Visier.

Gewissheit statt Vermutung

Die Frage lautet nicht länger: „Wurden wir schon angegriffen?“, sondern „Wie stark sind wir bereits unterwandert?“ und „Wurden unternehmenskritische Informationen abgezogen?“. Dies herauszufinden und dabei ein möglichst exaktes Bild des gesamten Ausmaßes wiederzugeben, ist keine leichte Aufgabe. Oft ist die Datenbasis zu gering, wurden Logdaten nur lückenhaft erfasst und zu schnell wieder gelöscht oder mit Malware infizierte Systeme sofort mit neuem Image bestückt, bevor überhaupt eine Analyse stattfand. Es fehlt an intelligenten Tools, an Zeit und an professionellen Forensikern.

Entwickelt für den Ernstfall

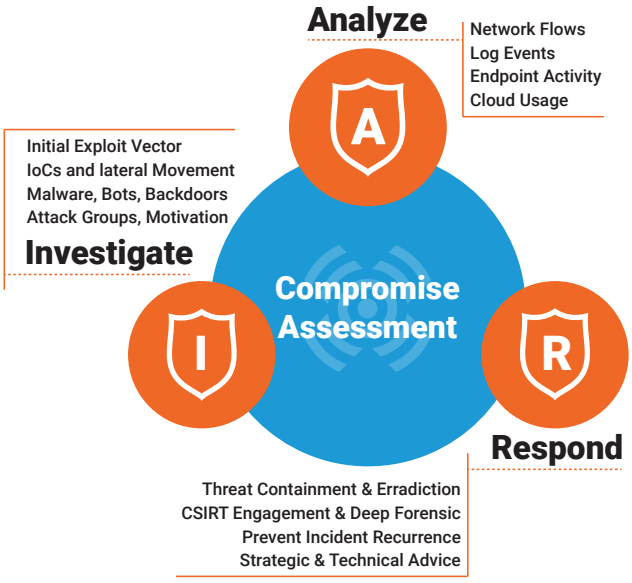
SecureLink's Compromise Assessment ist ein einzigartiger Service, der Organisationen ermöglicht, ihre IT-Infrastruktur auf Anwesenheit, Spuren und Aktivitäten professioneller Angreifer zu überprüfen. Unser auch als Infiltration Test bezeichneter Service hat dazu beigetragen, dass Organisationen unterschiedlichste, teilweise schwerwiegende Fälle von Industriespionage identifizieren konnten, die in manchen Fällen schon seit Monaten andauerten und zum Verlust geistigen Eigentums und finanziellen Schäden führten.

Erfahrung sichert Erfolge

Unsere Erfahrungen basieren auf der täglichen Analyse von Angriffen in unserem Advanced Cyber Defence Center (A.C.D.C.) und einer Vielzahl durchgeführter Compromise Assessments, bei denen wir Reconnaissance-Verhalten, Malware, Bots, Backdoors, CnC-Kommunikation, Datenausleitungen usw. mit hoher Zuverlässigkeit aufspüren konnten und regelmäßig verschiedenste Indikatoren (IoC) in allen Phasen eines gezielten Angriffs, auch als Attack Live Cycle oder Cyber Kill Chain bezeichnet, erkannten.

Unsere Erfahrungen

- Umfassende Kenntnisse von Werkzeugen, Taktik und Praktiken der Angreifer aus hunderten analysierter Vorfälle und der täglichen Praxiserfahrung im 24x7-Betrieb unseres eigenen CDC
- Dedizierter Threat Investigator für Koordination, Kommunikation und Qualitätssicherung
- Einsatz modernster Spitzentechnologie zur Erfassung und Untersuchung von Logs, Verkehrsflüssen, Anomalien und Artefakten
- Interdisziplinäre Teams für sofortigen Notfalleinsatz und alle auftretenden Eventualitäten, u.a. Malware Analyse, Incident Response und Forensik
- Intensiver Wissenstransfer mit Incident Response Teams aus weiteren 4 CDCs der SecureLink



Pentesting ist der falsche Ansatz

Traditionelle Methoden wie Penetration Testing, liefern hier keine hinreichenden Antworten, denn allein die Kenntnis möglicher Angriffsvektoren sagt nichts darüber aus, ob diese auch für Angriffe verwendet wurden und an welchen Stellen sich Angreifer festgesetzt haben. Wenn Pentester die intrinsischen Vertrauensbeziehungen von IT-Systeme untereinander nicht analysieren, können sie keine Aussagen über Angriffspfade treffen. Pentester arbeiten aufgrund ihres Business Cases naturgemäß mit Toolsets, die weit entfernt vom „Qualitätsstandard“ der Werkzeuge professioneller Hackersyndikate sind.

SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00

www.securelink.de

SecureLink is the market leading provider of cyber security in Europe.

SAFELY ENABLING BUSINESS

COMPROMISE ASSESSMENT

Mit diesem erprobten Ansatz sind wir in der Lage, sowohl ein- und ausgehenden Internetverkehr, als auch Inter-Segment-Verkehr innerhalb des Netzwerkes auf IoCs zu erfassen und zu analysieren. Dabei werden typische Host-Peer-Beziehungen in Clustern zusammengefasst und die normalen Interaktionen durch Baselining ausgefiltert. Davon abweichende Verhaltensweisen kommen ans Licht, weil die typischen Muster der eingesetzten Ausbreitungstechniken (Brute Force, Replication, Kerberos-Accounts-Scans, Power Shell Scripting, SQL-Injection, usw.) mit hoher Wahrscheinlichkeit identifiziert werden können.

Methodik & Systematik

Unser Analystenteam unter der Leitung eines Threat Investigators stimmt mit Ihnen im Detail die Vorgehensweise und wichtige Fragen z.B. die Platzierung der Sensoren ab. Ein wesentliches Element ist dabei auch das Verständnis Ihres Geschäftsmodells, Ihrer Assets und der Verkehrsmatrix.

Nachfolgend installieren wir technische Systeme zur Logdatenerfassung, Verkehrsflussanalyse, Erfassung von Endpunkt-Aktivitäten und der Nutzung von Cloud (Shadow) Applikationen.

Durch die Verwendung unterschiedlicher Technologien und Auswerteverfahren inklusive maschinellem Lernen schaffen wir die Basis für unsere Untersuchungen. Dabei versuchen wir den Impact auf Ihren operativen Systembetrieb so klein wie möglich zu halten.

Durch die Einbeziehung sicherheitsrelevanter Logdaten und die Erfassung und Korrelation von Aktivitäten am Endpunkt, mit externen Threat Intelligence Informationen können wir oftmals weitere wichtige Indikatoren entdecken. Dabei geht es uns immer um die Erfassung des Gesamtbildes bestehend aus Indikatoren, Schadensfall, Täterbild und Motivation.

Auf Basis dieser Informationen entwickelt unser Expertenteam ein präzises Bild der gegenwärtigen Bedrohungssituation, so dass Ihr CISO / CIO daraus unmittelbar ableiten kann, welchen Risiken Ihre Organisation aktuell ausgesetzt ist und welche Sofortmaßnahmen u.U. einzuleiten sind.

Über einen Zeitraum von 4 Wochen informiert Sie unser Expertenteam in wöchentlichen Status-Updates über die gefundenen Infektionen, Infiltrationen, Datenausleitungen usw. und gibt bei schwerwiegenden Vorfällen oder unklarer Disposition sofortige Rückmeldung.

Am Ende des Zeitraumes erarbeiten wir einen aussagekräftigen Abschlussbericht dessen Ergebnisse wir Ihrem Security-Team vorstellen. Je nach Situation unterbreiten wir Ihnen dabei strategische und technische Vorschläge für Maßnahmen, um zu verhindern, dass Angreifer erneut eindringen oder sich ähnliche Vorfälle unmittelbar wiederholen können.

Im Falle von unvorhersehbaren Notfalleinsätzen steht Ihnen unser Notfallteam (C.S.I.R.T.) mit Forensikern und Threat Respondern zur Verfügung.

Antworten

Das Compromise Assessment liefert Ihnen Antworten auf essentielle Fragen Ihres Risikomanagements.

- Welche Anzeichen von Angriffen existieren in meinem Netzwerk?
- Gibt es laufende Angriffe und welche sind das?
- Welche Gefahr geht von gefundener Schadsoftware und eventuellen Hintertüren aus?
- Welche Sofortmaßnahmen (Beweismittelsicherung, Memory Dumps, Malware Analyse, Sperrung von Accounts, Quarantäne von Systemen, Trennen von Kommunikationsbeziehungen) sind erforderlich?
- Wie kann verhindert werden, dass sich die Angriffe unmittelbar wiederholen?

Ergebnisse

Bei akutem Angriffsverdacht und ungewöhnlichen Anzeichen erhärtet oder entkräftet das Compromise Assessment Ihre Vermutung:

- Nachweis der Aktivitäten professioneller Angreifer
- Feststellung installierter Schadsoftware
- Identifikation von Motiv und Ursprung der Angriffe
- Aufdeckung persistenter Hintertüren auf Endsystemen
- Nachweis von initialem Angriffsvektor und lateraler Ausbreitung über kompromittierte Systeme / Accounts
- Soforthilfe und Notfalleinsatz
- Strategische Beratung und technische Unterstützung

COMPROMISE ASSESSMENT ist eine unkonventionelle, innovative und zeitgemäße Maßnahme des Risikomanagements, die Ihnen wirklich Gewissheit verschafft.

SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00