TruIntelligence™
Security Knowledge Network

Ein Netzwerk von Ressourcen der Spitzenklasse

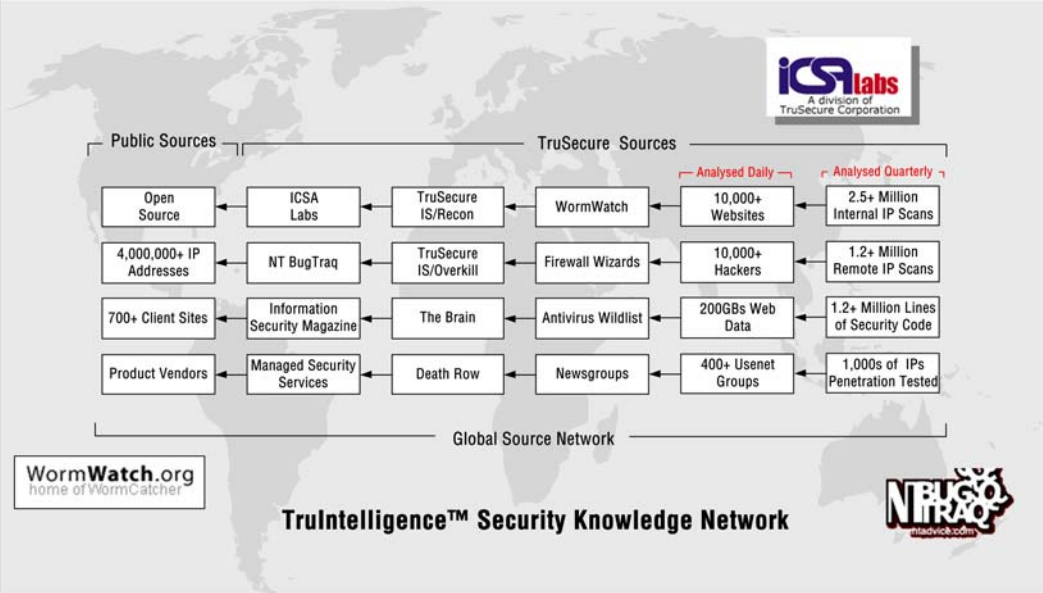
PRODUCT SHEET

TruIntelligence™, das Security Knowledge Network bildet die Basis für alle Services und Produkte von TruSecure. Dieses Netzwerk für Risikoforschung und vorausschauende Sicherheitsaufklärung versammelt einige der weltbesten Experten und unterhält eine der umfangreichsten Wissensbasen. Teil dieses Netzwerks sind die weltbekannten ICSA Labs™, die zentrale Autorität für die Zertifizierung von Sicherheitsprodukten.

Das TruIntelligence Netzwerk verfügt über vielfältigste öffentliche und nicht-öffentliche Quellen und erhebt sicherheitsrelevante Daten in erheblichem Umfang. Aber erst die Interpretation und Korrelation dieser Rohdaten durch erfahrene Analysten machen aus ihnen brauchbare Informationen und Empfehlungen, kurz umsetzbare Intelligenz.

Im Rahmen von TruIntelligence hat TruSecure in den letzten Jahren ein Risiko-Register aufgebaut, das ständig aktualisiert wird. Dabei werden Risiken konsequent auf ihre potentiellen Auswirkungen und Eintrittswahrscheinlichkeiten untersucht, zu deren Berechnung spezielle Bedrohungsmodelle entwickelt wurden. Auf der Grundlage der über die Jahre gesammelten Vergleichsdaten und durch die vorausschauende Aufklärungsarbeit ist TruSecure wie kaum ein anderer in der Lage, die Risiken zu identifizieren, die eine tatsächliche Auswirkung auf das Business haben.

Die Bausteine des TruIntelligence-Netzwerks



- ICSA Labs™ - Die Labs setzen Standards für die Performance von Sicherheitsprodukten und zertifizieren 95% aller Produkte aus den Bereichen Anti-Virus, Firewall, Intrusion Detection, IPSec und Kryptographie. Darüber hinaus verfügen die ICSA Labs über die wohl kompletteste und aktuellste Sammlung von Viren, Würmern, trojanischen Pferden und hacking tools sowie von anderen bösartigen Programmen oder Skripten.
- TS Intel – TruSecure's Organisation für Aufklärung („Intelligence") verfügt über eine gewaltige Datenbasis mit vielfältigsten Sicherheitsinformationen aus offenen Quellen, genannt Overkill. In Overkill befinden sich mehr als 1,6 Millionen Dokumente und ein Usenet-Archiv mit sicherheitsrelevanten Informationen, auch aus der „gray hat"-Szene. Dazu kommen täglich mehr als 200 GB Internetverkehr von über 130.000 verschiedenen News-Groups und anderen Internet-Quellen.
- NT BugTraq – Eine 1997 gegründete Sicherheitsgemeinde und Mailing-Liste, die mit heute mehr als 30.000 Abonnenten Sicherheitslöcher und „Exploits" in Betriebssystemen wie Windows NT, 2000 oder XP diskutiert.

TRUSECURE
Intelligent Risk Management

- IS/Recon (Internet Security Reconnaissance) – Seit 1996 unterhält TruSecure eine kontinuierlich arbeitende „Maulwurf-Organisation“ im Hacker-Untergrund. TruSecure verzeichnet täglich mehr als 500 Webseiten-„Hacks“ und andere Angriffe. In einer zentralen Datenbank, genannt „The Brain“, spürt TruSecure mehr als 10.000 Hackern und Hacker-Gruppen nach. In Fällen wie dem LoveBug-, Melissa- und Kournikova-Virus war IS/Recon instrumentell bei der Verfolgung der Straftäter.
- Security Operation Center (SOC) – Das TruSecure SOC analysiert rund um die Uhr Millionen Log-Einträge von Firewalls, IDS-Systemen und anderen Geräten aus Intra- und Extra-Nets.
- WormCatcher – TruSecure’s „Honeypot“-Netzwerk, das bei der Entdeckung von Code Red, Nimda und SQL Slammer führend beteiligt war.
- WildList – Die ICSA Labs unterstützen die WildList Organization International, der Computervirus-Informationsdienst, der beständig alle Exemplare von Viren und Würmern sammelt, die je weltweit eine Infizierung verursacht haben.
- Sicherheitskonsortien, Foren und Allianzen – TruSecure und die ISCA Labs haben engste Verbindungen bzw. moderieren zahlreiche wichtige Sicherheitsorganisationen wie das Firewall oder Anti-Virus Product Developer’s Consortium.

TruIntelligence - eine Erfolgsgeschichte

Das TruIntelligence-Netzwerk hat es TruSecure über viele Jahre ermöglicht, Angriffe Monate im Voraus akkurat vorauszusagen, seinen Kunden entsprechende Abwehrmaßnahmen rechtzeitig zu empfehlen und sicherzustellen, dass diese Maßnahmen mit der gewünschten Wirkung auch implementiert wurden.

- Melissa - TruSecure hat die notwendigen Abwehrmaßnahmen gegen den Melissa-Virus mehr als ein Jahr im Voraus seinen Kunden empfohlen.
- Love Letter - TruSecure hat VBS-Würmer mehr als ein Jahr im Voraus vorhergesagt und die entsprechenden Schutzmaßnahmen mehr als acht Monate bevor sich der Virus zeigte bei seinen Kunden implementiert. Von TruSecure geschützte Systeme waren von Love Letter deshalb nicht betroffen.
- DDoS - Vier Jahre bevor die ersten Distributed Denial of Service (DDoS) Attacken aufgetaucht sind, hat TruSecure sie allgemein beschrieben. Um dieser neuen Form der Bedrohung zu begegnen, gründete TruSecure im Jahre 1998 das ISP Security Consortium.
- Februar 2000 DDoS - Sechs Monate, bevor sie begannen, hat TruSecure diese verheerenden Angriffe spezifisch vorausgesagt. In der Zeit davor haben wir mehrere Treffen mit ISP‘s veranstaltet, die in der Gründung der Allianz für Internet Security resultierten.
- Code Red - Im Oktober 2000 hat TruSecure eine Alarmmeldung generiert, die drei Attackversionen gegen den IIS-Server ankündigte. TruSecure hat daraufhin eine einfache Konfigurationsempfehlung für den IIS-Server entwickelt, die unsere Kunden bei der Abwehr von Code Red half. Aufgrund dieser konsequenten Schutzstrategie und der vorausschauenden Aufklärung konnte Code Red keinen einzigen der von TruSecure zertifizierten Kunden schädigen.
- Nimda - Der Wurm benutzte vier Angriffsvektoren - vor Dreien schützte bereits die TruSecure Methodologie der wesentlichen Praktiken. Wir alarmierten unsere Kunden vor dem vierten Vektor im Februar 2001, 7 Monate vor dem Angriff. Während 68% vergleichbarer Unternehmen durch den Nimda-Virus infiziert wurden, waren dies bei den TruSecure-Kunden mit dem Enterprise-Zertifikat weniger als 0,5%.
- SQL-Slammer - Die TruSecure Methodologie und seine Empfehlungen schützte unsere Kunden vor dem Slammer-Angriff auch ohne das entsprechende Patching. TruSecure-Kunden mit dem Enterprise-Zertifikat waren von Slammer nicht betroffen.
- WebDAV/NTDLL.dll - Sieben Tage bevor die Angriffe begannen, warnte TruSceure seine Kunden vor Attacken über die WebDAV-Schwachstelle. Mit der Alarmierung kamen entsprechende Empfehlungen für Abwehrmaßnahmen.
- MSBlaster - TruSecure befragte 1.103 Unternehmen und fand, dass 20,9% dieser weltweiten Firmen durch den Blaster-Wurm infiziert waren, während nur 0,4% der TruSecure-Kunden mit dem Enterprise-Zertifikat betroffen waren.
- Sobig.F - Einer der sich am schnellsten verbreitenden Würmer hat mehr als 100.000 Computer infiziert, Millionen von E-Mails generiert und ganze Netzwerke lahm gelegt - in der Spitze war er für jedes 15. E-Mail verantwortlich, das weltweit gesendet wurde. Der Wurm hat keinen einzigen TruSecure-Kunden getroffen.

TruSecure Deutschland
Kaiserswerther Str. 115
D-40880 Ratingen
Tel: +49 (0)2102 420 765

TRUSECURE
Intelligent Risk Management
www.trusecure.com

040102PS-SKN