UNIVERSITY OF TWENTE.

PRESSEMITTEILUNG

Muster von DDoS-Angriffen erkennen

Zerstörerische Internetattacken finden und bekämpfen

Forscher der University of Twente geht neue Wege und sucht nach verdächtigen Mustern im Datenverkehr

Die rohe Wucht und Größenordnung der heutigen Attacken im Internet führen dazu, dass die klassische Überwachung kaum noch genügt – zumal die Anzahl miteinander verbundener Geräte in Zukunft drastisch zunehmen wird. Neue Wege sind daher gefragt: Rick Hofstede von der University of Twente (CTIT) verlässt mit seiner Doktorarbeit eingetretene Pfade und filtert die Angriffe heraus, die eine wirkliche Bedrohung darstellen. Seine neu entwickelte Open Source Software wird bereits weltweit von verschiedenen Organisationen verwendet. Seine Promotion ist übrigens ein „Joint PhD" mit der Universität der Bundeswehr in München.

Einfach eine große Zahl an Kombinationen von Benutzernamen und Passwörtern auszuprobieren, bis man diese gefunden hat – das kommt einem Angriff auf das Internet mit „roher Gewalt" gleich. Einmal „drin" im Computer des Users, kann er beispielsweise genutzt werden, um illegale Inhalte zu verbreiten oder die berüchtigten DDoS-Attacken loszutreten. Der ahnungslose User wird dadurch ungewollt selbst zu einem Angreifer.
Die Angriffe mit „roher Gewalt" geschehen über relativ anfällige Webanwendungen wie WordPress oder Joomla, aber auch über Secure Shell (SSH), wobei sich der Attackierende aus der Entfernung heraus in den Computer einloggen kann. Üblicherweise werden mögliche Attacken verhindert, indem der Netzwerkverkehr und die Logdateien auf jedem Computer analysiert werden. Diese klassische Herangehensweise zielt also vor allem auf den Inhalt des Datenverkehrs.

Hofstede setzt auf einen flowbasierten Ansatz

Das bedeutet jedoch, dass große Datenmengen analysiert werden, die keine Auswirkungen haben, erläutert Hofstede. Zumal der Schutz des Netzwerkes einer großen Organisation – mit zehntausenden Computern und Smartphones – durch den Blick auf das, was in jedem Gerät passiert, unmöglich ist.
Hofstede setzt dagegen auf einen flowbasierten Ansatz: Er sieht auf einem höheren Niveau nach den Datenströmen und sucht nach wiederkehrenden Mustern. So wie die Verbreitung eines Reklamefolders zu erkennen ist, ohne nach dem Inhalt des Folders zu sehen, erkennt er verdächtigen Internetverkehr an der Art und Weise

des Versendens und an dem Absender. Vorteilhaft ist, dass das an einem zentralen Punkt geschehen kann, beispielsweise bei einem Router, der den Internetverkehr regelt. Selbst wenn die Zahl der angeschlossenen Geräte zunimmt – und das ist durch den Aufstieg des Internets der Dinge zu erwarten –, ist dieser Schutz leicht handzuhaben. Hofstede beachtet nicht alle Angriffsversuche, sondern sucht nun nach der einen Attacke, die zur wirklichen Bedrohung führt, spricht das wahre Sicherheitsproblem, wo ein Eingreifen notwendig ist. Dank seines „Flow-basierten Gefährdungsschutzes" wird außerdem schneller erkannt, ob weitere Attacken von demselben Absender drohen.

Bis zu 100 Prozent Überwachungsgenauigkeit

Hofstede hat seinen Ansatz nicht nur in seinem Labor getestet, er hat seine dazugehörende Software SSHCure auch „open source" den „Computer Emergency Response Teams" verschiedener Organisationen zur Verfügung gestellt. Dabei stellte sich heraus, dass seine Methode erfolgversprechend ist und es zu deutlich weniger Vorfällen kommt. Die Überwachungsgenauigkeit betrug bis zu 100 Prozent – je nach Zahl der Anwendungen und abhängig vom Netzwerktyp. Zukünftige, leistungsfähigere Router können die Sicherung bereits selbstständig ohne Eingriff von Extra-Geräten übernehmen, erwartet Hofstede.

Joint PhD mit der Uni der Bundeswehr in München

Der Titel der Dissertation von Rick Hofstede lautet „Flow-based compromise detection". Seine Untersuchungen nahm er vor in der Gruppe „Design and Analysis of Communication Systems" mit Prof. Dr. ir. Aiko Pras als Doktorvater. Die Promotion ist ein „Joint PhD" mit der Universität der Bundeswehr in München. Hofstede ist inzwischen bei dem Internet-Sicherheitsunternehmen RedSocks beschäftigt.

Adresse:
University of Twente
Drienerlolaan 5
7522 NB Enschede

Pressekontakt für Journalisten aus Deutschland – *nicht zur Veröffentlichung*:

Gerne liefern wir Ihnen zusätzliches Bildmaterial und stellen für Sie Kontakt zu Ansprechpartnern bei der University of Twente her.

mediamixx GmbH
Alf Buddenberg
Tiergartenstraße 64
47533 Kleve
Tel.: 02821 - 711 56 13
E-Mail: alf.buddenberg@mediamixx.eu