

# Erfolg in der Früherkennung von Würmern

Zwei angehende Ingenieure der Communication Systems Group (CSG) der ETH Zürich haben in Kooperation mit Open Systems, einem führenden Anbieter von Managed-Security-Lösungen, eine Methode zur raschen Detektion von Computerwürmern entwickelt. *Martin Bosshardt*



**Martin Bosshardt**  
CEO der Open Systems AG seit 2002, schloss an der ETH Zürich mit Vertiefung an der Today Tokio als Elektroingenieur ab. Danach arbeitete er für ABB in Asien sowie als Geschäftsleitungsmitglied für Futurecom interactive in Zürich. Open Systems, ein führender Anbieter von Managed-Security-Lösungen, betreibt mit 25 Mitarbeitern Sicherheitsdispositive in über 70 Ländern auf fünf Kontinenten. [www.open.ch](http://www.open.ch)

Am 26. Januar 2003 infizierte der Computerwurm «SQL Slammer» innert 10 Minuten 75 000 Hosts weltweit. Der Datenverkehr, den der Wurm beim Suchen nach neuen Zielhosts generierte, legte ganze Firmennetzwerke lahm. Slammer war nicht der erste Computerwurm, der weltweit einen beachtlichen Schaden anrichtete: Seit dem ersten bekannten Fall, dem «Morris-Wurm» im Jahre 1988, ist die Zahl neuer Würmer und damit das Bedrohungspotenzial massiv angestiegen. Alleine im Jahr 2003 wurden 114 855 Zwischenfälle registriert. Experten schätzen den Schaden für die Unternehmen auf 55 Milliarden Dollar.

## Würmer überlasten Firmennetzwerke

Häufig wird von einem Computerwurm eine bestimmte Sicherheitslücke genutzt, die einen Host verwundbar macht. Ist ein Host infiziert, sucht er seinerseits das Internet nach neuen verwundbaren Hosts ab, um diese ebenfalls zu infizieren. Die Kettenreaktion ist ausgelöst. Vom Firmennetzwerk aus wird das Internet nach neuen Opfern abgesucht, was zu einer hohen Auslastung des internen Netzwerkes und in den meisten Fällen zum totalen Ausfall der Internetverbindung führt. Würmer bedrohen also die Verfügbarkeit der Netze, auch wenn sie erfolglos angreifen und auf keinem Zielrechner Schaden anrichten. Allein schon das erfolglose Scannen ist durch die resultierende Bandbreitenbelastung eine Bedrohung für die Netze und kann – insbesondere in einem globalen Netz – zu gewaltigen Schäden führen.

## Generische Detektionsmethoden sind gefragt

Die Früherkennung eines Wurmes in einem Firmennetzwerk kann die Ausbreitung ein-

dämmen und eine Überlastung der Infrastruktur verhindern. Die existierenden Programme, die den Netzwerkverkehr nach Würmern und Viren durchsuchen, basieren meistens auf der Methode des «Pattern Matching», der Erkennung von gewissen Mustern. Dabei wird der Inhalt jedes Paketes, das einen bestimmten Punkt im Netzwerk passiert, mit Mustern aus einer Virendatenbank verglichen. Gibt es Übereinstimmungen, wird das Paket verworfen und ein Alarm ausgelöst. Der grosse Nachteil:

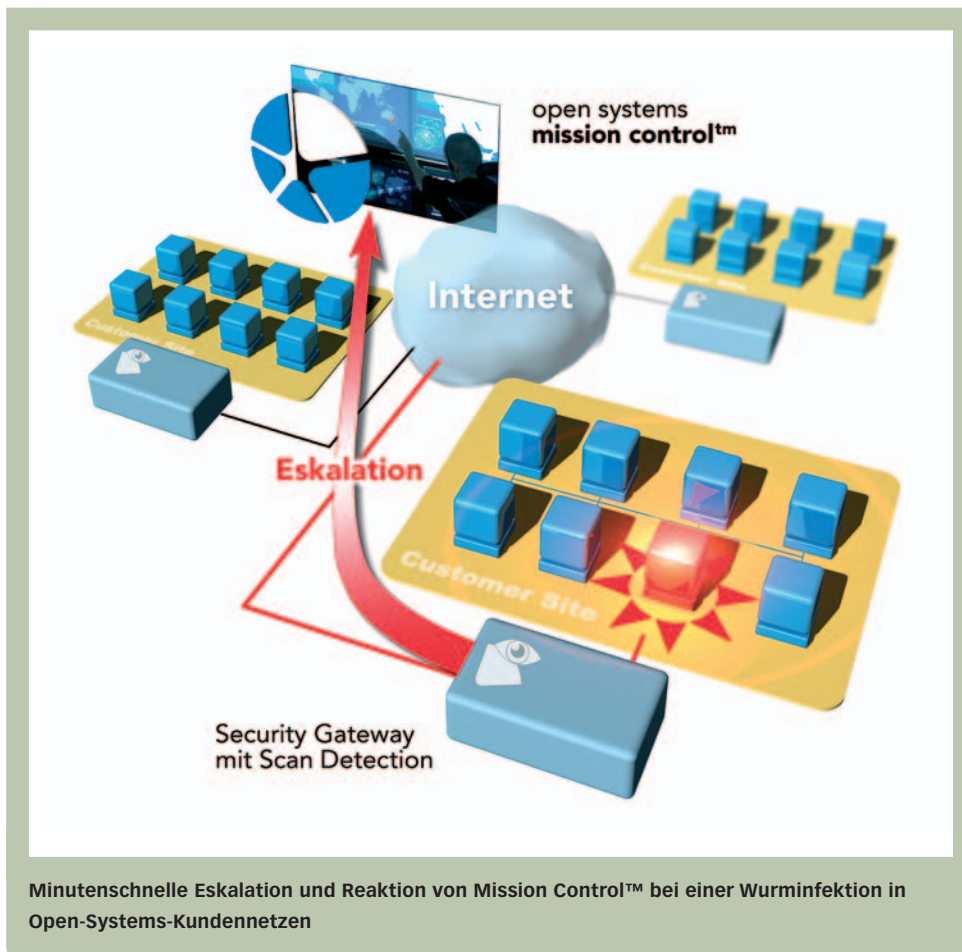
Diese Programme sind nur in der Lage, bekannte Würmer zu erkennen. Die Datenbank muss deshalb regelmässig aktualisiert und gewartet werden.

## Lösung der ETH Zürich geht neue Wege

Da neue Würmer aber immer häufiger und schneller auftauchen, steigt der Wunsch nach generischen Detektionsmethoden, die auch bisher unbekannte Würmer erkennen. Dadurch fällt die Wartung der Datenbank weg, was den finanziellen und den zeitlichen Aufwand deutlich reduziert.

Die Lösung, die Mitte April von den beiden angehenden Ingenieuren Christoph Göldi und Roman Hiestand im Rahmen des Forschungsprojektes DDoSVax der CSG bei Prof. Bernhard Plattner präsentiert wurde, geht neue Wege: Die Methode, die in enger Zusammenarbeit mit Open Systems, dem führenden Anbieter von Managed-Security-Lösungen entwickelt wurde, basiert primär auf der Analyse von fehlgeschlagenen Verbindungen. Ein Wurm sendet in den meisten Fällen eine riesige Menge von gleich oder ähnlich aussehenden Paketen ins Netzwerk, um nach verwundbaren Hosts zu suchen. Dieser «Scan Traffic» hat

«Würmer wecken den Wunsch nach generischen Detektionsmethoden.»



ein charakteristisches Aussehen, da viele der gewünschten Verbindungen nicht zustande kommen. Die fehlgeschlagenen Verbindungen sind ein klarer Hinweis auf eine Wurminfektion.

#### Dezentrale Überwachung – zentrale Auswertung

Die Anforderungen an generische Methoden sind hoch. Dazu gehört neben einfacher Wartbarkeit auch die Skalierbarkeit. Open Systems betreibt Sicherheitsinstallationen in über 70 Ländern für Kundennetze unterschiedlichster Grössen. Die Detektionsmethode muss deshalb sowohl in kleinen als auch in grossen Netzwerken angewendet werden können. Die Wurm detektion soll zudem mit der bereits bestehenden Hardware umgesetzt werden können, was Anforderungen an Prozessor und Speicherverbrauch stellt. Die von der CSG und Open Systems entwickelte Lösung funktioniert dezentral und basiert auf dem Prinzip der «Distributed Intrusion Detection», also einem Netzwerk mit eigener Intelligenz und proaktivem verteiltem Monitoring. Das auf der bestehenden Infrastruktur des Kun-

den, dem sogenannten Security Gateway, remote installierte Programm überwacht den Netzwerkverkehr. Wenn ein interner Computer infiziert wird und zu scannen beginnt, wird er sofort erkannt. Ein Alarm informiert die Sicherheitsingenieure von Mission Control™, dem rund um die Uhr, sieben Tage die Woche, besetzten Operation Center von Open Systems.

#### Mission Control™ reagiert umgehend

Die qualifizierten Sicherheitsingenieure des ITIL-zertifizierten Mission Control™ Center erstellen bei einer gemeldeten Bedrohung ein genaues Profil des infizierten Hosts. Informationen, wie zum Beispiel IP-Adresse, Ziel-Port und Scan-Rate, werden bereits auf dem Security Gateway gesammelt und an das Mission Control™ Center übermittelt. Dort werden sie analysiert, verifiziert und für den Kunden im Mission-Control™-Webportal sichtbar gemacht. Basierend auf diesen Informationen können die Mission Control™ Security Engineers mögliche Gegenmassnahmen ausarbeiten und schnell entsprechende Aktionen auslösen. Die Situationsbeurteilung durch Experten ist nach wie vor sehr wichtig,

da eine automatische Intervention zu Fehlabschaltungen führen könnte.

#### Geringe Fehlerquote

Fast so entscheidend wie eine kurze Detektionszeit ist die Anzahl Falschalarme, in der Fachsprache «False Positives» genannt. Jeder Falschalarm verursacht hohe Kosten, deshalb muss diese Messgrösse sehr tief gehalten werden. Neue Detektionsmethoden werden deshalb häufig an der Anzahl Falschalarme gemessen. Bei den ausführlichen Tests, die im Labor der CSG und bei Simulationen von Open Systems durchgeführt wurden, hat sich gezeigt, dass die neu entwickelte Methode praktisch keine Falschalarme auslöst.

#### Durchschlagender Erfolg in der Früherkennung

Die zuverlässige Identifikation von unbekanntem Angriffen ist mehr denn je erforderlich und zunehmend unternehmenskritisch. Neue und innovative Konzepte, Ansätze und Algorithmen sind gefragt. Die erfolgreiche neue Methode der CSG der ETH Zürich und von Open Systems beweist die Wirksamkeit der Zusammenarbeit von Forschung und Praxis. Die gefundenen Verteidigungsstrategien verzeichneten nicht nur im Labor durchschlagenden Erfolg: Die vielversprechende Methode wurde durch Open Systems mit Simulationsdaten sowie später mit realen, aufgezeichneten Traffic-Daten wiederholt getestet. Die Tests zeigten klar, dass die entwickelte Methode Computerwürmer innerhalb weniger Minuten detektiert. Open Systems plant, die neue Detektionsmethode in Kürze bei ihren Kunden einzuführen. Dank der fundierteren Eskalationsanalyse der neuen Algorithmen können die Spezialisten von Mission Control™ zukünftig noch schneller und konsequenter reagieren und entsprechende Interventionen einleiten. Distributed Intrusion Detection, also Netzwerke mit eigener Intelligenz und proaktivem verteiltem Monitoring, sind die Zukunft. Die Communication Systems Group (CSG) der ETH Zürich hat zusammen mit Open Systems einen grossen Schritt in diese Richtung unternommen. ■