**Zeitschrift:** Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

**Herausgeber:** Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

**Band:** 92 (2001)

**Heft:** 9

**Artikel:** Den Hackern auf der Spur

**Autor:** Wespi, Andreas

**DOI:** https://doi.org/10.5169/seals-855700

**Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

**Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

**Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

**Download PDF:** 12.07.2025

**ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch**

# Den Hackern auf der Spur

## «Intrusion Detection» als zusätzlicher Schutz

Der Angriff auf die Computer des World Economic Forum in Davos zeigt: Die Zahl von politisch oder ökonomisch motivierten Hackerangriffen steigt weiter an. So genannte Intrusion-Detection-Systeme (IDS) ergänzen bestehende Sicherheitsmassnahmen und bieten zusätzlichen Schutz vor Hackerangriffen. Dieser Artikel beschreibt, wie IDS funktionieren, und charakterisiert sie anhand von fünf Merkmalen.

*Andreas Wespi*

Die Idee, ein System zu bauen, das Hackerangriffe automatisch entdeckt, ist relativ alt. Das erste System wurde bereits im Jahre 1980 von James P. Anderson beschrieben [1]. Lange Zeit blieb es dann aber relativ ruhig um die neue Technologie. Noch vor fünf Jahren waren nur einige wenige kommerzielle IDS erhältlich. Diese Produkte waren hauptsächlich für Umgebungen mit sehr hohen Sicherheitsansprüchen gedacht und wurden beispielsweise von Regierungen oder von militärischen Organisationen zum Schutz ihrer Computersysteme eingesetzt.

Mit dem Wachstum des Internets ist auch eine Zunahme von Angriffen auf Computersysteme zu beobachten. Das belegen die jährlich publizierten Daten des amerikanischen Cert Coordination Center [2].

Computersysteme frei von Sicherheitslücken zu halten, ist unmöglich. Als Ergänzung zu den präventiven Massnahmen setzen immer mehr Unternehmen und Organisationen deswegen IDS ein, um Hackerangriffe zu entdecken. Die gestiegene Nachfrage hat mittlerweile zu einem Angebot von mehr als 20 verschiedenen IDS-Produkten geführt [3].

In diesem Artikel wird beschrieben, welche unterschiedlichen Varianten von IDS es gibt und nach welchen Kriterien sie sich unterscheiden lassen.

### Wie funktioniert ein IDS?

Ein IDS beobachtet fortlaufend den momentanen Zustand von Computern oder Netzwerken. Durch die Analyse relevanter Informationen sollen Angriffe von aussen und Angriffe, die sich innerhalb des Netzwerks abspielen, detektiert werden. Im ersten Fall spricht man gemeinhin von Hackerangriffen, während der zweite Fall dem Missbrauch von Privilegien durch berechtigte Computerbenützer innerhalb des eigenen Unternehmens entspricht. Ferner gilt es, nicht nur erfolgreiche Angriffe, sondern auch Angriffsversuche oder Vorstufen von Angriffen (z.B. wenn Informationen über ein potenzielles Angriffsziel gesammelt werden) zu erkennen.

Bild 1 zeigt schematisch die Architektur eines IDS. Abstrahiert kann ein IDS beschrieben werden als ein Detektor, welcher Daten analysiert, die vom zu beschützenden System kommen. Der Detektor kann auch aktiv Systemabfragen machen, um zusätzliche Informationen über den Systemzustand zu erhalten.

Der Detektor hat typischerweise Zugriff auf drei Arten von Daten:

- Audit-Daten, welche die momentane Systemaktivität beschreiben. Audit-Daten können z.B. die Logfiles eines Webservers oder eines Firewalls sein.
- Langzeitinformationen, welche das IDS für seine Analyse braucht. Ein Beispiel ist eine Datenbank mit den Signaturen (Merkmalen) bekannter Angriffe.
- Konfigurationsinformationen, welche Aufschluss über die Konfiguration des zu überwachenden Systems geben, wie z.B. die Beschreibung der Netzwerktopologie.

Die Aufgabe des Detektors ist nun, die eingehenden Daten zu analysieren und zu entscheiden, ob Anzeichen für einen Angriff vorliegen. In diesem Fall wird ein Alarm generiert, und eventuelle Gegenmassnahmen können automatisch eingeleitet werden.

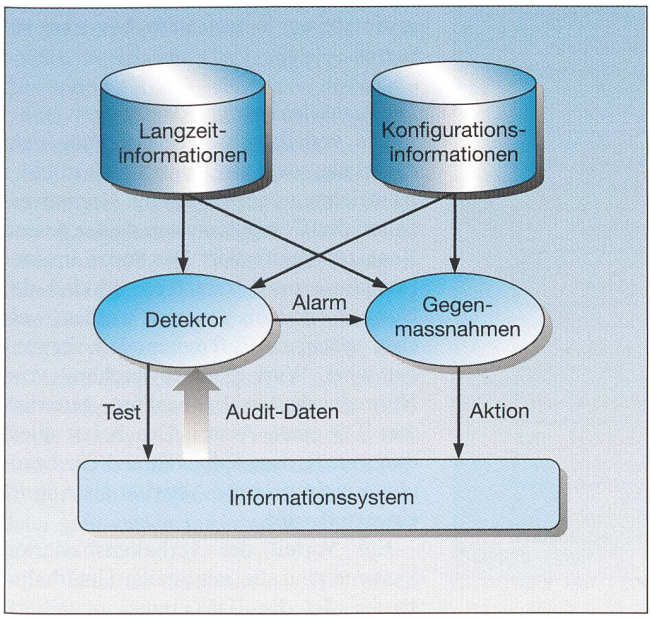


**Bild 1 Architektur eines IDS**
Das Detektionssystem erhält Daten von verschiedenen Komponenten des Computersystems. Falls ein Angriff erkannt wird, wird ein Alarm ausgelöst.

### Unterscheidungsmerkmale für IDS

Leider gibt es kein universelles IDS, das alle Typen von Angriffen zuverlässig entdecken kann. Demzufolge haben sich im Lauf der Zeit verschiedene Arten entwickelt. In der Vielfalt der Möglichkeiten, wie ein IDS zu bauen ist, liegt wohl auch die Tatsache begründet, dass Intrusion Detection auch als Forschungsgebiet sehr attraktiv ist und es neben den kom-

merziellen Produkten eine grosse Anzahl von Forschungsprototypen gibt [4].

Es gibt verschiedene Möglichkeiten, IDS zu klassifizieren. IDS lassen sich gemäss den fünf Kriterien, die in Bild 2 dargestellt sind und nachfolgend genauer beschrieben werden [5], charakterisieren.

**Host- oder netzwerkbasiert**

Als die ersten IDS konzipiert wurden, waren die Zielsysteme Grossrechner und deren lokale Benützer. Dies vereinfachte die Aufgabe des IDS stark, da Interaktionen mit externen Rechnern selten waren. Das IDS machte Gebrauch von den Logfiles, welche das Betriebssystem anlegte und die lokal auf dem Grossrechner zur Verfügung standen.

Als Grossrechner mehr und mehr durch Netzwerke von Workstations ersetzt wurden, passten sich die IDS dem veränderten Umfeld an und versuchten, Angriffe auch auf Netzwerkebene zu erkennen. Verschiedene Typen von Attacken lassen sich nämlich kaum detektieren, wenn nur lokale Logfiles analysiert werden. Ein Beispiel ist TCP-Hijacking (TCP = Transmission Control Protocol), bei dem ein Angreifer versucht, sich in eine bestehende Verbindung zwischen einem Client und einem Server einzuschalten und die Rolle des Servers zu übernehmen [6].

Generell kann man zwischen host- und netzwerkbasierten Systemen unterscheiden. Hostbasierte Systeme analysieren die Daten, welche lokal auf einem System zur Verfügung stehen. Solche lokale Datenquellen reichen von Audit-Logfiles, die vom Betriebssystem generiert werden, um sicherheitskritische Systemaufrufe zu erfassen, über Logfiles, die von Applikationen wie z.B. einem Webserver oder einem Firewall geschrieben werden, bis hin zu Daten, die über die Systemauslastung wie z.B. die Diskaktivität Auskunft geben.

*Hostbasierte IDS*

Hostbasierte IDS weisen den Nachteil auf, dass sie entweder auf der zu überwachenden Maschine installiert oder die Logfiles zur Analyse auf eine separate Maschine kopiert werden müssen. Im ersten Fall besteht das Problem darin, dass das IDS selber Ressourcen braucht, die dann den zu überwachenden Anwendungen nicht mehr zur Verfügung stehen, und im zweiten Fall, dass das Netzwerk mit dem Datentransfer stark belastet wird. Zudem sind Systemadministratoren in der Regel zurückhaltend, wenn es darum geht, zusätzliche Komponenten auf sicherheitskritischen Maschinen – und um die geht es in der Regel – zu installieren.

*Netzwerkbasierte IDS*

Netzwerkbasierte IDS analysieren den Datenverkehr und suchen nach Spuren von Attacken in den Datenpaketen. Sie werden vor allem in «Shared»-Netzwerken eingesetzt, wo jede angeschlossene Station den gesamten Datenverkehr eines Netzwerksegments sehen kann. Der Vorteil von netzwerkbasierten IDS besteht unter anderem darin, dass das IDS auf einer eigenen Maschine installiert werden kann und somit die bestehende Infrastruktur nicht belastet. Netzwerkbasierte Systeme sind allerdings nicht für «Switched»-Netzwerke geeignet, da hier das IDS in der Regel jeweils nur die Verbindung zwischen zwei Hosts analysieren kann. Auch bei verschlüsseltem Datenverkehr ist ein netzwerkbasiertes IDS wenig hilfreich.

**Wissens- oder verhaltensbasiert**

IDS können auch anhand ihrer Detektionsmethode unterschieden werden.

*Die wissensbasierte Methode*

Die wissensbasierte Methode beruht auf den charakteristischen Merkmalen von bereits bekannten Angriffen. Die Systeme lösen Alarm aus, sobald der Systemzustand mit den in einer Datenbank abgelegten Beschreibungen von bekannten Angriffen übereinstimmt. Somit ist ein wissensbasiertes IDS stark abhängig von einer genauen und umfassenden Beschreibung möglicher Angriffe.

Die Vorteile dieser Methode liegen darin, dass – zumindest in der Theorie – die Fehlalarmrate tief ist und die Alarmmeldungen aussagekräftig sind. Das IDS kann genau sagen, welcher Angriff beobachtet wurde und welche Beobachtungen zur Auslösung eines Alarms führten. Ein gravierender Nachteil wissensbasierter IDS ist jedoch, dass nur bekannte Angriffe detektiert werden können. Neue Angriffe, für die das IDS noch über keine Signatur verfügt, können nicht entdeckt werden. Ein weiterer Nachteil besteht darin, dass es sehr aufwändig ist, das Wissen über bekannte Angriffe auf dem neuesten Stand zu halten. Die Erfahrung zeigt, dass pro Woche fünf bis zehn neue Sicherheitslücken bekannt werden. Oftmals gibt es zudem verschiedene Wege, diese Sicherheitslücken auszunutzen, und die Signaturen der entsprechenden Angriffe können je nach Betriebssystem variieren.

*Die verhaltensbasierte Methode*

Die verhaltensbasierte Methode geht davon aus, dass ein Angriff sich in einer Abweichung vom erwarteten Normalverhalten des Computersystems oder dessen Benützer manifestiert. Das heisst, in einer Lernphase muss zuerst ein Modell des Normalverhaltens generiert werden, welches später als Referenzmodell verwendet wird. Wird eine Abweichung vom Normalverhalten beobachtet, generiert das IDS einen Alarm. Das heisst allerdings auch, dass jede während der Lernphase nicht gelernte Aktivität als Angriff eingestuft wird.

Ein Vorteil der verhaltensbasierten Systeme sind die minimalen Unterhaltskosten. Ist das IDS einmal installiert,

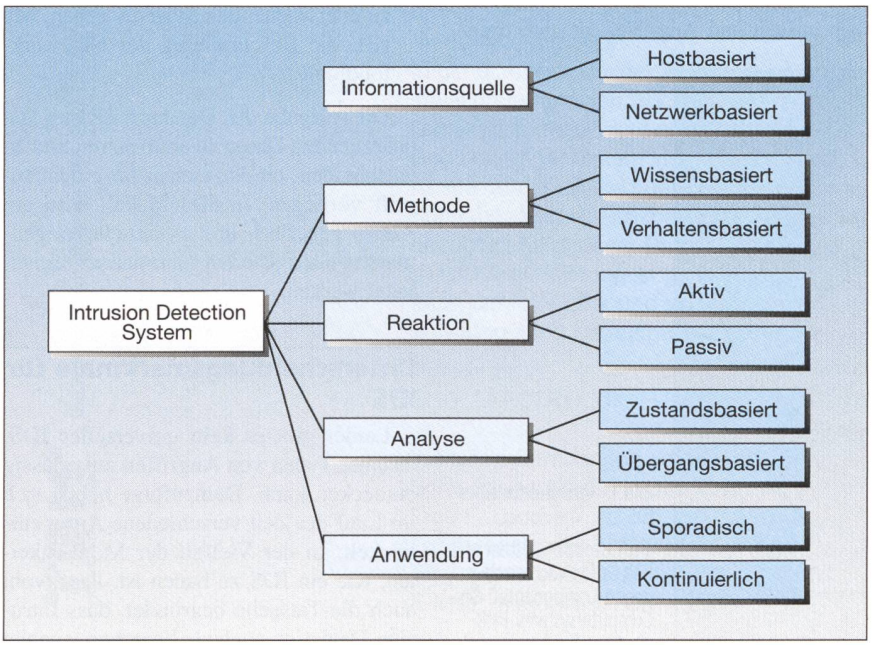


**Bild 2 Fünf Möglichkeiten, nach denen IDS klassifiziert werden können**

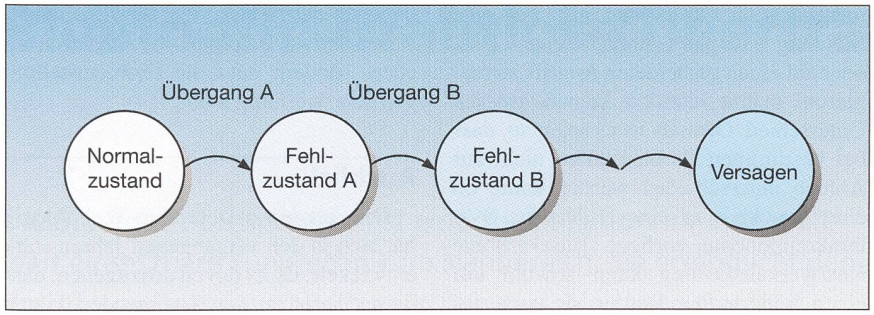


**Bild 3 Angriffe können an bestimmten Zuständen oder an Übergängen zwischen Zuständen erkannt werden.**

muss es nicht andauernd mit neuen Signaturen versorgt werden. Ein grosser Nachteil besteht aber darin, dass verhaltensbasierte IDS eine hohe Fehlalarmrate aufweisen. Es gibt jedoch neuere Forschungsergebnisse, die zeigen, dass es möglich ist, verhaltensbasierte IDS zu bauen, welche zuverlässig funktionieren. Die zurzeit auf dem Markt erhältlichen IDS-Produkte sind aber praktisch ausschliesslich wissensbasiert.

### Aktiv oder passiv

Die meisten IDS sind passiv. Wenn ein Angriff entdeckt wird, generieren die Systeme lediglich eine Fehlermeldung. Einige wenige IDS sind aktiv, das heisst, sie verfügen über die Fähigkeit, automatisch Gegenmassnahmen einzuleiten. Eine mögliche Gegenmassnahme wäre beispielsweise die Umkonfiguration des Firewalls, um die Netzwerkverbindung des Angreifers zu unterbinden.

Es könnte fatal sein, wenn ein IDS basierend auf einem Fehlalarm irrtümlich eine Gegenmassnahme einleitet.

### Zustands- oder übergangsbasiert

Man kann zwischen zwei Detektionsparadigmen unterscheiden. Die eine Klasse von IDS analysiert Zustände, die andere untersucht Übergänge zwischen Zuständen. Bild 3 veranschaulicht die beiden Paradigmen anhand von Begriffen aus der Zuverlässigkeitstheorie.

Fehlzustand A und Fehlzustand B repräsentieren zwei Glieder in einer Kette von Ereignissen, welche letztlich zu einem Ausfall oder Versagen des Systems führen. Fehlzustand A kann etwa bedeuten, dass eine fehlerhafte Anwendung installiert wurde, und Fehlzustand B, dass es einem Angreifer gelungen ist, mittels der fehlerhaften Anwendung an eine Kopie der Passwortdatei zu kommen. Der Endzustand kann dann sein, dass ein Angreifer sich mittels der in der Passwortdatei gefundenen Information eingeloggt hat.

Im Idealfall detektiert das IDS einen Angriff, bevor es zu einem Systemausfall kommt. Systematisch betrachtet haben IDS die folgenden Möglichkeiten, einen Angriff zu erkennen:

- Das IDS versucht zu bestimmen, ob sich das System im Normalzustand befindet. Dies bedingt aber, dass es eine Definition des Normalzustandes gibt. Wie bereits bei den verhaltensbasierten Systemen diskutiert wurde, ist es schwierig, den Normalzustand zu definieren. Ein weiterer Nachteil besteht darin, dass keine genaue Beschreibung des Problems geliefert werden kann, falls das System nicht im Normalzustand ist. Das Wissen, dass sich das System nicht mehr im Normalzustand befindet, hilft wenig, wenn es darum geht, das Problem zu beheben.
- Das IDS kann Fehlzustände erkennen. In der Regel ist es einfacher, einen Fehlzustand als den Normalzustand zu beschreiben. Das Problem besteht aber darin, eine umfassende Beschreibung aller möglichen Fehlzustände zu haben.
- IDS können Übergänge erkennen, welche zu einem Fehlzustand führen. Zum Beispiel kann ein netzwerkbasiertes System nach speziellen Ereignissen Ausschau halten, von denen man weiss, dass sie zu einem Fehlzustand oder zum Systemausfall führen.

### Sporadisch oder kontinuierlich

*Sporadische IDS*

Ein IDS kann sporadisch den Momentanzustand eines Systems analysieren. Tests dazu sind z.B. die Überprüfung, ob die neuesten Sicherheitsupdates installiert sind oder ob Benützer Passwörter gewählt haben, die nicht leicht zu erraten sind, oder ob Konfigurationsdateien modifiziert wurden. Die Werkzeuge, um solche Tests auszuführen, sind als Konfigurations-Checker bekannt und weit verbreitet. Sie bieten aber nur bedingt Schutz vor Hackern, da immer nur Momentaufnahmen des Systems analysiert werden. Angriffe werden deswegen oft nicht oder nur verspätet erkannt. Zudem gibt es Hacker-Tools, die es dem Angreifer erlauben, die in Logfiles hinterlassenen Spuren automatisch zu löschen, damit bei der nächsten Konfigurationsüberprüfung keine Verdachtsmomente entdeckt werden.

*Kontinuierliche IDS*

Kontinuierliche IDS überwachen das System in Echtzeit mit dem Ziel, Angriffe möglichst umgehend zu entdecken. Wenn man heutzutage von Intrusion Detection spricht, so meint man in der Regel kontinuierliche IDS, welche rund um die Uhr aktiv sind. Es sollte aber auch nicht ausser Acht gelassen werden, dass es nicht nur darum geht, einen Angriff zu detektieren, sondern auch darum, auf die Attacke zu reagieren. Intrusion Detection in Echtzeit nützt wenig, wenn die Reaktion auf den Angriff nur mit grosser Verzögerung erfolgt.

## Noch bestehen viele Probleme

Obwohl die Weiterentwicklung der IDS in den vergangenen paar Jahren stetig vorangetrieben wurde, bestehen heutzutage immer noch eine Reihe offener Probleme.

### Hohe Fehlalarmrate

Die Fehlalarmrate von kommerziellen Produkten ist immer noch relativ hoch. Dafür gibt es verschiedene Gründe. Zum einen kann ein IDS auf Grund der analysierten Informationen oftmals nicht eindeutig entscheiden, ob ein Angriff vorliegt. Im Bestreben, keinen Angriff zu verpassen, wird im Zweifelsfall eine Alarmmeldung ausgegeben.

IDS müssen oft eine grosse Menge an Audit-Daten verarbeiten. Für Echtzeitsysteme heisst dies, es muss sichergestellt werden, dass die Daten möglichst schnell analysiert werden. Um dies zu erreichen, werden die Signaturen einfach und möglichst generisch gehalten. Zu starke Vereinfachungen führen ebenfalls zu Fehlalarmen.

### Fehlende Standardisierung

Heutzutage verwendet praktisch jedes IDS seine eigene Syntax für Alarmmeldungen. Es sind Bestrebungen im Gange, das Format der Alarmmeldungen zu standardisieren. Weiter ist man daran, die Namen aller bekannten Sicherheitslücken zu vereinheitlichen [7]. Das ist mit einem grossen Aufwand verbunden, weil praktisch täglich neue Sicherheitslücken bekannt werden.

### Intrusion-Detection-Management

Die Spezialisierung der IDS führt dazu, dass für einen unternehmensweiten

Schutz verschiedene Typen von IDS eingesetzt werden. Dies bedingt aber auch, dass die IDS und, noch wichtiger, die Alarmmeldungen, welche die IDS generieren, verwaltet werden müssen. Somit wird eine Managementsoftware benötigt, welche es dem Systemadministrator erlaubt, an einer zentralen Konsole alle Alarmmeldungen zu bearbeiten. Im Idealfall sollte pro Angriff nur eine einzige Meldung auf der Konsole erscheinen, unabhängig davon, wie viele IDS die Attacke sehen.

**Integration mit System- und Netzwerkmanagement**

Intrusion-Detection-Management hat sehr viele Gemeinsamkeiten mit System- und Netzwerkmanagement. An Stelle von Sensoren, welche z.B. die Diskaktivität oder die Netzwerkauslastung messen, müssen Sensoren verwaltet werden, die Angriffe erkennen. Beide Sensortypen senden Meldungen zu einer Managementkonsole. Ob es nun gilt, auf eine Meldung bezüglich einer defekten Disk oder auf einen gemeldeten Angriff zu reagieren, macht letztlich keinen grossen Unterschied. Oftmals ist es sogar so, dass bei bestimmten Problemfällen nicht auf Anhieb unterschieden werden kann, ob eine Attacke oder eine fehlerhafte Systemkomponente vorliegt. Eine erhöhte Netzwerkauslastung kann sowohl auf einen fehlerhaften Router als auch auf eine Denial-of-Service-Attacke hindeuten.

**Rückverfolgung des Angreifers**

TCP/IP, das Netzwerkprotokoll des Internets, erlaubt keine zuverlässige Identifikation des Absenders eines Datenpakets. Deshalb ist es sehr schwierig, den Ursprung einer Attacke zu lokalisieren.

Dies ist nur eine Auswahl von offenen Problemen. Sie soll zeigen, dass Intrusion Detection nicht nur darin besteht, Systeme zu entwickeln, die Logfiles analysieren und nach Spuren von Angriffen suchen, sondern dass die Problemstellungen sehr vielfältig sind.

## Ausblick

Die Intrusion-Detection-Technologie hat sich in den vergangenen Jahren stark entwickelt. Es ist davon auszugehen, dass dieser Trend in den kommenden Jahren anhält. Insbesondere dürfte die Benutzerfreundlichkeit der Systeme im Mittelpunkt der Entwicklungsanstrengungen stehen.

Trotz aller Technologie sollte nicht ausser Acht gelassen werden, dass Intrusion Detection auch ein organisatorisches Problem ist. Es müssen Strukturen geschaffen werden, damit möglichst rasch und richtig auf Angriffe reagiert werden kann. Da die meisten IDS nur Alarmmeldungen generieren, braucht es immer noch einen Sicherheitsexperten, der bei einem Angriff die notwendigen Gegenmassnahmen einleiten kann.

## La chasse aux pillards

Les «Intrusion Detection Systems» (IDS) sont destinés à déceler les attaques contre les systèmes et réseaux d'ordinateurs. Les premiers systèmes ont déjà été développés au cours des années quatre-vingts mais n'ont connu une plus grande diffusion qu'après l'avènement d'Internet. Aucun système ordinateur n'est exempt de lacunes de sécurité et c'est pourquoi de plus en plus d'entreprises et organisations ont recours à un IDS en complément des mesures préventives.

Il existe différents types d'IDS. Un important critère de distinction est la source de laquelle les systèmes puisent leurs informations. Les IDS à base «hôte» cherchent des traces d'attaque dans des fichiers «log», écrits par exemple par le système d'exploitation. Les IDS à base réseau sont directement reliés au réseau et analysent le trafic de données. Autre critère de distinction: la méthode. Les IDS à base cognitive cherchent les traces d'attaques connues et sont tributaires d'une description précise et complète d'attaques possibles. Les IDS basés sur le comportement définissent d'abord le comportement normal d'un système ou d'un utilisateur puis cherchent dans le service opérationnel les écarts importants par rapport au comportement normal.

La technologie de détection d'intrusion fait l'objet d'un développement constant. Les principaux problèmes consistent à minimiser les faux alarmes et à accroître la convivialité.

## Referenzen


[1] *J.P. Anderson:* Computer Security Threat Monitoring and Surveillance, Fort Washington, PA, 1980.

[2] CERT/CC Statistics 1988–2000, http://www.cert.org/stats/certstats.html

[3] *K. Jackson:* Intrusion Detection System Product Survey, Research Report LA-UR-99-3883, Los Alamos National Laboratory, June 1999.

[4] *M. Sobirey:* Intrusion Detection Systems Page, http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html

[5] *H. Debar, M. Dacier, A. Wespi:* A Revised Taxonomy for Intrusion-Detection Systems, Annals of Telecommunication, Vol. 55, No. 7–8, Paris, July/August 2000.

[6] *S. Northcutt:* Network Intrusion Detection: An Analyst's Handbook, New Riders Publishing, Indianapolis, Indiana, 1999.

[7] Common Vulnerabilities and Exposures, http://www.cve.mitre.org/


## Adresse des Autors


IBM-Forschungslabor, 8803 Rüschlikon: Dr. *Andreas Wespi*, anw@zurich.ibm.com