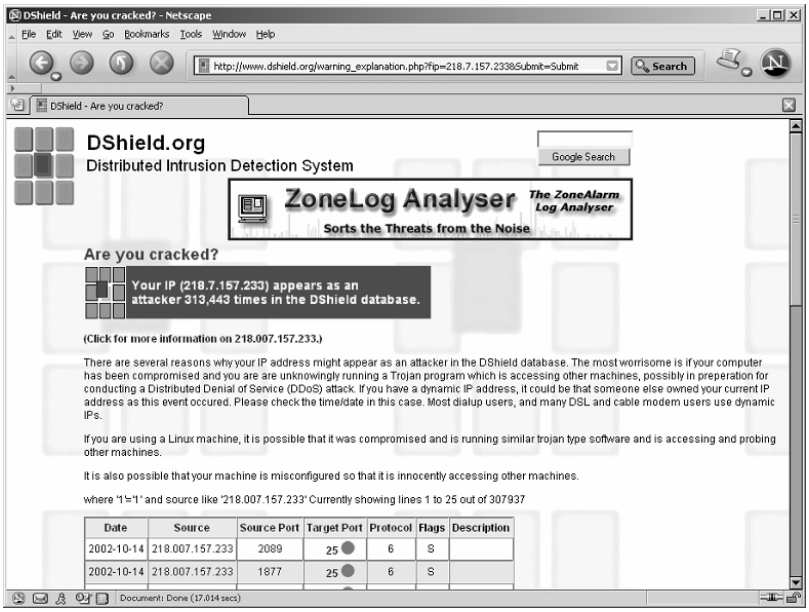

Abb. 3-1 Intrusion-Mapping-System dshield.org

3.5 Incident Detection: Ein Vorfall wird gemeldet

Zusätzlich zu den in Kapitel 3.4 genannten Anzeichen eines Angriffs kommt es gerade in größeren und weit verstreuten Organisationen vor, dass Meldungen über mögliche Sicherheitsvorfälle telefonisch erfasst werden oder ein IDS-Alarm beim lokalen Systemadministrator abgeklärt werden muss. Es ist wichtig, im Vorfeld zu wissen, welche Informationen man dann erfragen sollte. Eine Checkliste mit standardisierten Fragen gehört daher unbedingt in ein Sicherheitsvorfall-Behandlungskonzept.

Meldung des Vorfalls

Merkblatt vorbereiten

Es ist für die erste Einschätzung der Situation wichtig, dass die Person, die die Meldung entgegennimmt, bereits die richtigen Dinge erfragt. Wenn die meldende Person diese Informationen nicht sofort zur Hand hat, sollten diese möglichst schnell nachgeliefert werden. Es gilt hier aber der Grundsatz, dass Informationen, die nicht frühzeitig erfasst werden, häufig niemals erfasst werden. Jeder Mitarbeiter, der möglicherweise eine Vorfallsmeldung entgegennehmen könnte, sollte auf einem Merkblatt die nachfolgend erläuterten Fragen griffbereit haben. Zur besseren Vorbereitung der eigenen Mitarbeiter in der Organisation können auch fertige Formulare bereitgehalten werden. Diese For-

mulare gehören auf jeden Fall auch in den User Help Desk, für den Fall, dass dort eine Erstmeldung aufläuft. Allerdings sollte dafür auch entsprechend geschultes Fachpersonal vorgehalten werden. Der Hinweis, hier nicht in Panik zu verfallen, ist zwar bei professionellem Herangehen überflüssig, kann aber nicht oft genug gegeben werden.

Allgemeine Informationen

Daten, die auf jeden Fall für die Dokumentation eines Sicherheitsvorfalls erfasst werden sollten, sind

- aktuelle Uhrzeit
- Wer oder welches System berichtet den Vorfall?
- Art und Wesen des Vorfalls
- vermuteter Zeitpunkt des Vorfalls
- mittelbar und unmittelbar betroffene Hardware und Software
- Kontaktstelle für das Incident-Response-Team und die Ermittler

Informationen über den Anrufer

Die erste Information für alle an der Ermittlung beteiligten Personen ist: Wer hat wann von wo angerufen? Für mögliche weitere Nachfragen sollte die meldende Person unbedingt E-Mail-Adresse und Telefonnummer hinterlassen.

Als Nächstes sollte gefragt werden, wie und durch wen der Sicherheitsvorfall entdeckt wurde. Wichtig ist in diesem Zusammenhang auch, wann der Vorfall bemerkt wurde. Äußert der Anrufer Vermutungen darüber, wann der Vorfall seiner Meinung nach stattgefunden hat, sind auch diese zu berücksichtigen.

Für spätere Entscheidungen und auch für die Bewertung des Angriffsziels sollte die meldende Person die direkten und indirekten Auswirkungen auf das Unternehmen oder die Organisation beschreiben. Hierbei sollte auch nachgefragt werden, ob sich in Form einer Kettenreaktion der mögliche Schaden potenzieren könnte. Wenn sich bereits Aussagen über entstandenen oder möglicherweise entstehenden finanziellen Schaden treffen lassen, kann dies mitunter zur weiteren Motivation bei Entscheidungsträgern führen.

Für die weitere Kommunikation sollte festgelegt werden, welche Personen für weitere Informationen kontaktiert werden sollen. Dies betrifft sowohl eine Kontaktperson, die den Ermittlern für weitere Zwischenfragen oder lokale Unterstützung zur Verfügung steht, als auch die Möglichkeit, dass sich die betroffene Organisation an einer zentralen Stelle über den Stand der Ermittlungen informieren kann.

Informationen vom betroffenen System

Für die eigentliche Untersuchung sind nähere Informationen über das betroffene System oder den Systemkomplex sehr wichtig. Hierzu zählen Informationen über Hardware, Betriebssystem und Anwendungssoftware. Um allerdings den Zustand des Systems nicht unnötig zu verändern, sollten dies Informationen offline, d.h. nicht vom betroffenen System selbst, erlangt werden. Weiterhin ist zu klären, ob auf diesem System vertrauliche oder anderweitig kritische Daten gespeichert oder verarbeitet werden. Ist das System Bestandteil eines kritischen Geschäftsprozesses? Wer sind die Hauptanwender dieses Systems? Wer sind die Hauptadministratoren des Systems, wie können sie erreicht werden? Wo ist das System physisch positioniert? Kann sichergestellt werden, dass keine unberechtigten Personen physischen Zugriff auf dieses System haben?[4] Zur besseren Beurteilung der Situation sollte erfragt werden, in welchem Zustand sich das System befindet. Ist es eingeschaltet oder ausgeschaltet? Was steht auf dem Bildschirm oder der Konsole? usw.

Diese Informationen sind zwar für die erste Lagebeurteilung wesentlich, die Erfahrung zeigt aber, dass man oft auch ohne diese Hinweise auskommen muss. Oft ist nicht bekannt, wo sich ein System physisch genau befindet, wie es funktioniert und für welche Geschäftsprozesse es relevant ist. Außerdem muss berücksichtigt werden, dass sich die meldende Person nicht immer in einem ausgeglichenen Zustand befindet oder genügend Zeit hatte, alle wichtigen Informationen in Ruhe mitzuteilen.

Informationen über den Angreifer

Wenn bereits Informationen über einen potenziellen Angreifer vorliegen, sollten diese ebenfalls bei der Meldung erfasst werden. Ist der Angreifer noch aktiv? Gibt es Anzeichen für einen Denial-of-Service-Angriff? Wurden Systeme oder Daten manipuliert oder zerstört? Gibt es erste Vermutungen über einen Innen- oder Außentäter? Diese Informationen sollten die Ermittler aber sorgfältig überprüfen.

4. Mitunter sollten die Sicherheitsverantwortlichen sofort bestimmen, dass außer den unmittelbar an der Ermittlung beteiligten Spezialisten niemand den Raum mit den betroffenen Systemen betreten darf, da die Gefahr der Zerstörung wichtiger Spuren besteht. Dies ist besonders wichtig, wenn der Eigentümer des betroffenen PC oder ein Systemadministrator selbst verdächtigt wird.

Was wurde bereits unternommen?

Damit eingeschätzt werden kann, welche Spuren auf dem System vom Angreifer oder von einem übereifrigen Administrator hinterlassen wurden, ist es wichtig herauszufinden, welche Tätigkeiten am betroffenen System bereits vorgenommen wurden. Wurde das System heruntergefahren? Wurde die Netzverbindung getrennt? Wurden bereits lokale Audit- bzw. Protokolldaten analysiert? Wurden in Folge des Angriffs bereits Modifikationen am System vorgenommen? Im Hinblick auf eine mögliche Spurenbeseitigung sollte geklärt werden, welche internen und externen Personen bereits informiert wurden. Ist spezielle Netzwerk- oder Systemaudit-Software im Einsatz?

Abhängig davon, welche Informationen bei der Erstmeldung erfasst wurden, wirkt sich dies auf den personellen und finanziellen Aufwand zur Lösung des Problems aus. Die Dauer eines möglichen Ausfalls des Systems und des zu unterstützenden Geschäftsprozesses kann ebenfalls davon abhängen. Nachdem alle erreichbaren Informationen aufgenommen und diese an den verantwortlichen IT-Mitarbeiter übermittelt wurden, muss er feststellen, ob es sich eventuell nur um »falschen Alarm« handelt.

3.6 Sicherheitsvorfall oder Betriebsstörung?

Eine der wesentlichen Erkenntnisse bei der Behandlung eines möglichen Sicherheitsvorfalls ist die Frage, ob es sich um ein wirkliches Sicherheitsproblem handelt oder anders formuliert: Handelt es sich wirklich NICHT um eine Betriebsstörung?

Zu Beantwortung dieser Frage gehört neben den benötigen aktuellen Statusinformationen auch eine gewisse Kenntnis der Organisation, der zugrunde liegenden IT-Landschaft und der dort tätigen Mitarbeiter. Sicherlich ist es nicht immer ratsam, sich zu lange mit der Entscheidungsfindung, ob es sich um einen Sicherheitsvorfall handelt, zu beschäftigen. Manchmal ergeben sich auch erst während der laufenden Ermittlung konkrete Anhaltspunkte, dass es sich doch nicht um einen Sicherheitsvorfall handelt.

Fehlalarm?

Um Klarheit zu gewinnen, sollten alle Hinweise auf mögliche Fehler in Anwendung, System oder Hardware soweit durchleuchtet werden, dass sie ausgeschlossen werden können. So lassen sich z. B. veränderte Zeitstempel von wichtigen Systemdateien möglicherweise auf ein kürzlich eingespieltes Update zurückführen. Ebenso können scheinbar beeinträchtigte Netzwerkressourcen nicht nur Folge eines Denial-of-Service-Angriffs sein, sondern ursächlich mit gestarteten Applikatio-