Ordnung zum Betrieb eines Frühwarnsystems (FWS) im Datennetz der Technischen Universität Dresden

Vom 09.11.2009

Aufgrund von § 13 Abs. 5 des Gesetzes über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz – SächsHSG) vom 10.12.2008 (SächsGVBl. S. 900) hat das Rektorat der TU Dresden folgende Ordnung beschlossen:

Präambel

Die zunehmende Professionalisierung der Internetkriminalität erhöht das Gefahrenpotential für den Missbrauch von Rechen- und Kommunikationssystemen der TU Dresden. Missbrauch erzeugt negative Auswirkungen auf Personen und Geschäftsprozesse der Universität. Die Folgen eines Missbrauchs sind u.a. Image-Schäden für die Universität (negative Innen- und Außenwirkung), finanzielle Schäden (z.B. Verlust von forschungsrelevanten Daten oder Kosten für die Wiederherstellung eines Systems), Beeinträchtigung der Aufgabenerfüllung, Beeinträchtigung der persönlichen Unversehrtheit und Verstöße gegen gesetzliche Bestimmungen, Verträge und Vorschriften. Zur signifikanten Erhöhung der Sicherheit im Datennetz der TU Dresden ist deshalb die Einführung eines Frühwarnsystems notwendig.

§1
Zweck des Frühwarnsystems

(1) Der Betrieb des FWS im Datennetz der TU Dresden erfolgt gemäß § 14 Abs. 6 sowie Abs. 10 der Rahmenordnung für die Nutzung der Rechen- und Kommunikationstechnik und Informationssicherheit an der TU Dresden (IuK Rahmenordnung) ausschließlich zum Erkennen, Eingrenzen bzw. Beseitigen von Störungen oder Fehlern und zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung an rechen- und kommunikationstechnischen Einrichtungen und Systemen der TU Dresden.

(2) Die Erhebung und Verwendung von anderen Nachrichteninhalten ist unzulässig.

(3) Den nach § 3 Verpflichteten ist es untersagt, sich oder anderen über das für die Erbringung der Dienste nach IuK-Rahmenordnung einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für die in Abs. 1 genannten Zwecke verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit diese Ordnung oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. Darüber hinaus ist die Übermittlung von personenbeziehbaren Daten aus dem FWS nur im Rahmen der juristischen Auskunftspflicht und ausschließlich zu Zwecken nach § 13 Abs. 2 Nr. 3 SächsDSG zulässig.

(4) Die Verwendung der verarbeiteten Daten zur Verhaltens- oder Leistungskontrolle von Beschäftigten und/oder Studenten sowie die Zusammenführung von Daten zu Verhaltens- bzw. Persönlichkeitsprofilen ist unzulässig und findet nicht statt.

§ 2
Geltungsbereich

Das FWS umfasst den Geltungsbereich nach § 1 Abs. 1 und Abs. 3 der IuK Rahmenordnung. Für andere Einrichtungen nach § 1 Abs. 2 IuK Rahmenordnung sind mit den jeweiligen Einrichtungen gesonderte Vereinbarungen notwendig.

§ 3
Verantwortlichkeiten

(1) Die Verantwortung für die Installation, Wartung und den Betrieb des FWS sowie für die Verwaltung der verarbeiteten Daten und die Vergabe von Zugriffsrechten liegt beim ZIH. Mit der Wahrnehmung der Aufgaben zur Erfüllung der Zwecke nach § 1 Abs. 1 werden nach § 6 SächsDSG auf das Datengeheimnis verpflichtete Mitarbeiter des ZIH (Security Incident Response Team) sowie die nach § 15 Abs. 3 IuK benannten Administratoren der Struktureinheiten beauftragt.

(2) Dem IT-Sicherheitsbeauftragten der TU Dresden obliegt als IT-Sicherheitsbeauftragtem des ZIH die Vergabe/Löschung der Zugriffsrechte. Über die Vergabe und Löschung der Zugriffsrechte führt der IT-Sicherheitsbeauftragte ein Protokoll.

§ 4
Erfassung und Verarbeitung der Daten

(1) Es werden folgende Verkehrsdaten verarbeitet:

- Status der Verbindung, Netzprotokoll, Datenrate, Zeitraum der Verbindung
- Daten der Verkehrsbeziehung
    - Quell- und Ziel-IP-Adresse
    - Quell- und Ziel-Port
    - Technische Parameter der Verbindung (siehe Anlage 1)

(2) Das FWS bezieht seine Daten von den zentralen Netzknoten (Backbone-Router) im Datennetz der TU Dresden und insbesondere vom X-WIN Übergang zum Deutschen Forschungsnetz mittels der NetFlow-Technologie (siehe Anlage 1). Die Daten werden in einer Datenbank des FWS (siehe Anlage 2) gespeichert. Die Verarbeitung der Daten erfolgt automatisiert durch das FWS. Die aufgezeichneten, detaillierten Verkehrsdaten werden am übernächsten Arbeitstag nach Speicherung automatisch durch das FWS gelöscht.

§ 5
Zugriffsrechte

(1) Der Betrieb des FWS erfolgt im ZIH. Das ZIH setzt nach § 6 SächsDSG auf das Datengeheimnis verpflichtete Mitarbeiter (Security Incident Response Team) ein.

(2) Die Administratoren der Struktureinheiten besitzen ausschließlich Zugriffsrechte auf die zusammengefassten Meta-Ereignisse ihrer Zuständigkeitsbereiche (verantwortliche Datennetze).

Meta-Ereignisse des FWS sind z.B.:

- Anomalien, wie z.B. High Target Index, High Concern Index
- High Traffic Index
- Massives Port-Scanning, ICMP-Flooding, Port-Flooding
- Wurm-Aktivitäten eines Systems

(3) Das Security Incident Response Team des ZIH hat folgende Berechtigungen:

- Konfiguration, Management und Betrieb des FWS
- Einsichtnahme in die vom FWS zusammengefassten Meta-Ereignisse
- Einsichtnahme in die personenbeziehbaren Verkehrsdaten im FWS

(4) Der Zugriff auf die personenbeziehbaren Verkehrsdaten nach § 4 ist nur zulässig zu den in § 1 Abs. 1 genannten Zwecken und erfolgt nur aus begründetem Anlass.

(5) Für den Zugriff sind mindestens zwei Mitglieder des Security Incident Response Team des ZIH erforderlich (4-Augen-Prinzip).

(6) Sofern möglich, ist der betroffene Nutzer über den Zugriff im Voraus, in jedem Fall jedoch im Nachhinein, zeitnah detailliert zu unterrichten. Zur Aufklärung und Unterbindung von Missbräuchen kann, bis zur Zweckerreichung nach § 11 Abs. 3 IuK die Information des Nutzers unterbleiben. Für einen Missbrauch (z.B. Spam-Versand, Denial-of-Service, unberechtigter Zugriff auf ein geschütztes System) müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen.

(7) Der Anlass und die Einsichtnahme sind zu dokumentieren. Über eine beabsichtigte Einsichtnahme in die eindeutig personenbeziehbaren Verkehrsdaten ist im Regelfall vorab, in jedem Fall im Nachhinein, der Datenschutzbeauftragte zu hören. Dieser kann eine Einsichtnahme sowie die weitere Verwendung für Zwecke nach § 1 Abs. 1 untersagen, wenn überwiegende schutzwürdige Interessen des Betroffenen einer Nutzung entgegenstehen.

§ 6
Protokollierung

(1) Der Zugriff auf das FWS und insbesondere auf die personenbeziehbaren Daten wird protokolliert.

(2) Der Zugriff auf die personenbeziehbaren Daten wird mit folgenden Daten protokolliert:

- Personen, die den Zugriff durchführen
- Zweck des Zugriffs
- Eingeleitete Maßnahmen
- Datum des Zugriffs
- Ergebnis des Zugriffs

(3) Es gelten insbesondere die einschlägigen Bestimmungen der IuK-Rahmenordnung.

(4) Das jeweils aktualisierte Zugriffsprotokoll ist unverzüglich dem Datenschutzbeauftragten zuzuleiten.

§ 7
Festlegungen zur allgemeinen Datensicherheit

Die Festlegungen zur allgemeinen Datensicherheit sind im IT-Sicherheitskonzept in Anlage 3 beschrieben.

§ 8
Vorgehensweise zu Zwecken nach § 1 Abs. 1

(1) Bei zentral durch das ZIH verwalteten Ressourcen, z.B. WLAN, werden betroffene Systeme in eine Quarantäne gesetzt und der Nutzer informiert.

(2) Bei Systemen, die in der Verantwortung von Administratoren nach § 15 Abs. 3 IuK stehen, ist der zuständige Administrator verpflichtet bei festgestellten Meta-Ereignissen (Anomalien) die Sachlage zeitnah zu klären und das ZIH entsprechend zu informieren. Wird in angemessener Zeit keine Klärung herbeigeführt, ist das ZIH berechtigt, die entsprechende IP des Systems bzw. das Datennetz in eine Quarantäne zu setzen. Der zuständige Administrator veranlasst die Freischaltung des betroffenen Systems bzw. Datennetzes aus der Quarantäne in eigener Verantwortung.

(3) Bzgl. der Information betroffener Nutzer gelten insbesondere die Bestimmungen nach § 14 Abs. 5 und 7 der IuK Rahmenordnung.

§ 9
Veröffentlichung, Inkrafttreten

(1) Diese Ordnung tritt am Tage nach Veröffentlichung in den Amtlichen Bekanntmachungen der TU Dresden in Kraft.

(2) Diese Ordnung ist ausgefertigt aufgrund des Beschlusses des Rektorats der TU Dresden vom 27.10.2009.

Dresden, den 09.11.2009
Der Rektor

Prof. Hermann Kokenge

Anlage 1 NetFlow

NetFlow ist eine ursprünglich von Cisco entwickelte Technik zur Sammlung und Auswertung von Informationen über IP-Netzverkehr.

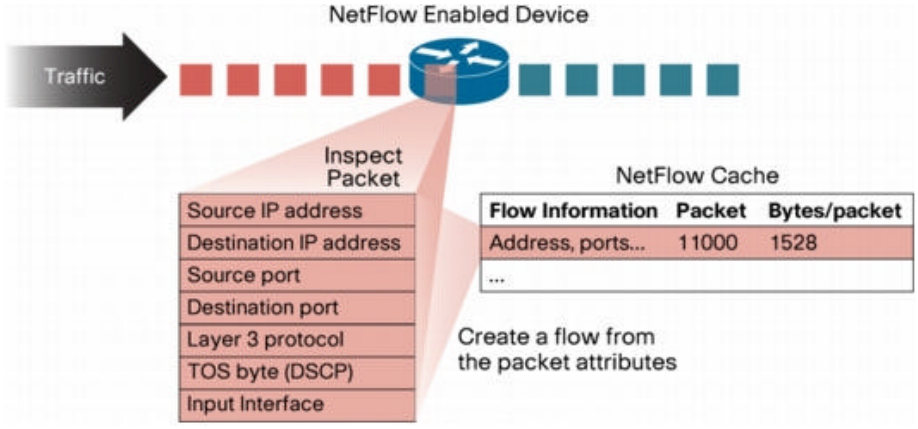
NetFlow basiert auf Flows. Ein Flow ist definiert als eine unidirektionale Sequenz von IP-Paketen, die alle mindestens die folgenden 7 gleichen Werte besitzen:

1. Quell-IP-Adresse
2. Ziel-IP-Adresse
3. Quell-Port für UDP bzw. TCP, 0 für andere Protokolle
4. Ziel-Port für UDP bzw. TCP, Typ und Code für ICMP, 0 für andere Protokolle
5. IP Protokoll
6. Ingress Interface
7. IP Type of Service

NetFlow existiert in verschiedenen Versionen. Das FWS der TU Dresden verwendet NetFlow Version 9, das in RFC 3954 standardisiert beschrieben ist. NetFlow Version 9 bietet weitere technische Verkehrsinformationen, die im FWS der TU Dresden gesammelt werden:

- Quell- und Ziel-VLAN
- MPLS-Informationen
- Verwendete Netzwerk-Interfaces der Kommunikationsbeziehung
- Minimum und Maximum TTL des Flows
- Minimum und Maximum Paketgröße des Flows

NetFlow wird auf Geräten der Netzwerkinfrastruktur, z.B. Routern, erzeugt. Das Gerät analysiert dazu den Netzverkehr und generiert aus den IP-Paketen die definierten Flow-Informationen.



Die gesammelten Daten werden als Flows im NetFlow-Cache des Gerätes gesammelt und als UDP-Datenstrom ausschließlich an den registrierten Kollektor versendet. NetFlow ist ein passives Verfahren, d.h. ohne den Netzverkehr aktiv zu beeinflussen.

Anlage 2 Lancope Stealthwatch NBA System

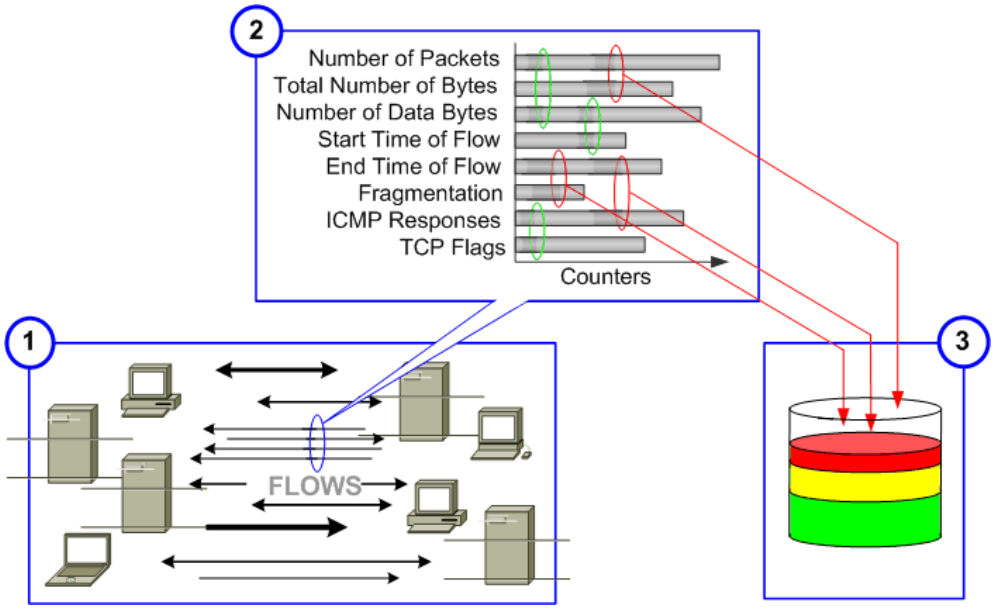
Die TU Dresden setzt als Frühwarnsystem im Datennetz das Network Behavior Analysis (NBA) System *Stealthwatch* der Firma Lancope ein. Das *Stealthwatch*-System ermöglicht eine signifikant schnellere Reaktion auf Sicherheitsvorfälle und Anomalien im Datennetz. Systeme der TU Dresden, die durch einen Sicherheitsvorfall (z.B. Infizierung mit einer Schadsoftware) beeinträchtigt werden bzw. andere Systeme beeinträchtigen, sollen schnellstmöglich und eindeutig identifiziert und ggf. der Aufwand sowie die Kosten zur Wiederherstellung gesenkt werden.

Das *Stealthwatch*-System lernt automatisch das Netzverhalten der Systeme im Datennetz der TU Dresden durch Analyse der Verkehrsdaten, die von den Netzknoten (Backbone-Routern) mittels NetFlow geliefert werden (1).

Signifikante Abweichungen im Netzverhalten werden durch spezielle Algorithmen im System erkannt und mit einem Punkte-System bewertet (2), wie z.B.:

- High Traffic Index
- High Target Index (Denial-of-Service)
- Probes (Port-Scans, ICMP Flooding, Suspect UDP Traffic)
- Ungewöhnlich hohe Anzahl an Flows

Abweichungen über einen definierten Schwellwert (Meta-Ereignisse) werden alarmiert (3).



Weiterhin erkennt das System Regelverstöße im Netzwerk (Policy Violations), z.B. nicht zugelassene Dienste bzw. Verkehrsbeziehungen.

Das Stealthwatch-System besteht aus einem Kollektor zum Sammeln der Flows (*Stealthwatch* Xe for NetFlow) und der *Stealthwatch* Management Console (SMC) zur Auswertung und Analyse der Informationen.

Das *Stealthwatch*-System ist mandantenfähig mittels eines dedizierten Rechte- und Rollenkonzepts, das unterschiedlichen Benutzern und Gruppen fein granulare Berechtigungen auf die Informationen sowie auf die Funktionen zuweisen lässt. Die Mandantenfähigkeit ermöglicht

die Einbindung der lokalen Administratoren der TU Dresden in das System.

Die Zusammenfassung von Abweichungen im Datennetz durch spezialisierte Algorithmen bietet insbesondere eine frühzeitige Erkennung von Zero-Day Angriffen.

Anlage 3 IT-Sicherheitskonzept

Stealthwatch-System

Der Zugriff auf die Informationen über die SMC bzw. auf den *Stealthwatch* Xe Kollektor erfolgt ausschließlich über das dediziertes Rechte- und Rollenkonzept im System. Das ZIH verwaltet dafür zentral administrierte Benutzerkennungen mit Passwortschutz. Die Server sind nur über einen gesicherten HTTPS-Kanal (Server-Zertifikate im Rahmen der DFN PKI) zugänglich. Das Betriebssystem der Stealthwatch Server ist ein minimales, von Lancope gehärtetes, Linux. Die *Stealthwatch* Server werden im Rechenzentrum (Trefftz-Bau) des ZIH betrieben, der Zugang zu diesem Raum ist nur registrierten, zugelassen Mitarbeitern des ZIH gestattet. Die Server befinden sich in einem verschlossenen Serverschrank. Weiterhin ist eine Frontblende mit Schloss-System installiert, um die Festplatten der Server vor unbefugtem Zugriff zu sichern.

Netzkonzept

Der Betrieb des *Stealthwatch*-Systems erfolgt in einem nur innerhalb des IP-Adressraumes der TU Dresden erreichbaren Subnetzes. Das Subnetz ist durch eine vom ZIH administrierte Access-Liste geschützt. Der Zugriff auf die SMC erfolgt nur von registrierten IP-Adressen und über speziell freigegebene Ports. Der Kollektor nimmt NetFlow-Informationen nur von den registrierten Backbone-Routern im Datennetz der TU Dresden an. Die Backbone-Router versenden die NetFlow-Informationen nur an den registrierten Kollektor. Die Backbone-Router werden ausschließlich von zugelassenen Mitarbeitern des ZIH über speziell freigegebene IP-Adressen und Benutzerkennungen mit Passwortschutz administriert (Management-Zugang).

Schutz der Clients

Die Visualisierung der Daten über die SMC erfolgt mittels einer Java-Rich-Client Applikation auf dem Client-PC des zugelassenen Mitarbeiters. Deshalb sind an den Client entsprechende Sicherheitsanforderungen zu stellen:

- Der Client-PC darf nur hinter einer zentral vom jeweiligen Administrator bzw. vom ZIH administrierten Firewall betrieben werden.
- Auf dem Client-PC sind eine lokale Software-Firewall und ein Virenscanner zu installieren.
- Der Zugriff über die Java-Rich-Client Applikation darf nur von einem Benutzerkonto ohne Administratorrechte erfolgen.
- Vom Administrator des Clients wird sichergestellt, dass die jeweils aktuellen Patches für das Betriebssystem und für die installierten Anwendungen zeitnah eingespielt werden.
- Der Client-PC darf keine Dienste anbieten.