CERT NRW

Jahresbericht 2012

Inhalt

Einleitung

Nachfolgend gibt das Computer Emergency Response Team der Landesverwaltung Nordrhein Westfalen (CERT NRW) einen Bericht über seine Tätigkeiten im Jahr 2012 ab. Der Bericht enthält Informationen über identifizierte Schwachstellen in IT-Verfahren und Webangeboten sowie über Sicherheitsvorfälle, die durch das CERT NRW untersucht wurden. Darüber hinaus enthält der Bericht eine Einschätzung der Entwicklung der Bedrohungslage und dem Stand der Informationssicherheit in der Landesverwaltung.

Aufgaben des CERT NRW

Das CERT NRW hat den Auftrag, Behörden und Einrichtungen des Landes mit sicherheitsrelevanten Informationen zu versorgen und bei entsprechenden Vorfällen Hilfestellung zu leisten. Das CERT NRW übernimmt primär folgende Aufgaben in der Landesverwaltung:

- Informationen zu neuen Schwachstellen und Bedrohungen der IT-Sicherheit
- Handreichungen und Handlungsempfehlungen zum Schutz vor Bedrohungen der IT-Sicherheit
- Hilfestellung bei Sicherheitsvorfällen
- Koordination von Informationsfluss und Gegenmaßnahmen bei Sicherheitsvorfällen
- Technische Vorfallsanalyse
- Schulungen und Workshops

Darüber hinaus überwacht das CERT NRW bei IT.NRW ausgewählte Bereiche der Infrastruktur mit Hilfe von [redacted]

Des Weiteren führt das CERT NRW Schwachstellenscans und Sicherheitstests durch und berät in verschiedenen grundsätzlichen IT-Sicherheitsfragen.

Tätigkeitsbericht

Die Grundlage für die Tätigkeiten des CERT NRW bildet das „Konzept für ein Computer Emergency Response Team Nordrhein-Westfalen - CERT NRW - “ in der jeweils aktuellen und mit dem Auftraggeber abgestimmten Version sowie die in der Dienstleistungsvereinbarung beschriebenen Konkretisierungen hierzu.

In 2012 wurden entsprechende Dienstleistungen erbracht, wobei aufgrund zahlreicher IT-Sicherheitsvorfälle der Schwerpunkt eindeutig im Bereich der Sicherheit von Webangeboten lag. Einzelheiten hierzu können den nachfolgenden Beschreibungen entnommen werden.

Schwachstellen in Webangeboten der Landesverwaltung NRW

[redacted]

Sicherheitsrelevante Meldungen

Im Jahr 2012 hat das CERT NRW 961 Advisories des CERT-Bund weiter geleitet und 27 eigene Advisories bzw. Sicherheitsmeldungen über die CERT-Info Mailingliste zur Verfügung gestellt. Die durch das CERT NRW selbst erstellten Advisories haben dabei Schwachstellen aufgegriffen, die für die Landesverwaltung relevant waren und vom CERT-Bund nicht oder erst deutlich später gemeldet wurden bzw. dienten als Ergänzung der Advisories des CERT-Bund.

Tickets

Insgesamt hat das CERT NRW im Jahr 2012 616 Security Incident Tickets bearbeitet (Advisories sind hier nicht enthalten), wobei die meisten händisch erstellt wurden.

Security Incident Tickets werden erstellt für

- Schwachstellenfunde
- IT-Sicherheitsvorfälle
- sicherheitsrelevante Anfragen an das CERT aus der Landesverwaltung NRW
- sicherheitsrelevante Anfragen oder Hinweise von extern (Bürger, CERT-Bund, CERT-Verbund und andere)

Sicherheitsvorfälle

Als IT-Sicherheitsvorfälle werden Ereignisse behandelt, die zu Verlust eines oder mehrerer der grundlegenden Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit führen oder bei denen eines oder mehrere der oben genannten Schutzziele akut gefährdet sind.

Dazu zählen

- ernstzunehmende oder erfolgreiche Angriffe auf Systeme und Anwendungen
- gravierende Schwachstellenfunde

Angriffe, die täglich in großer Zahl auftreten (Massenphänomene) aber keine echte Bedrohung darstellen, da die angegriffenen Systeme dafür nicht verwundbar sind, werden nicht als Sicherheitsvorfall gewertet.

Nicht alle zunächst als Sicherheitsvorfall gewertete Ereignisse bestätigen sich im Nachhinein als solcher. Der umgekehrte Fall kann ebenfalls eintreten.

Nachfolgend wird eine Liste der wichtigsten Sicherheitsvorfälle aufgeführt, die das CERT NRW im Jahr 2012 untersucht und bearbeitet hat.

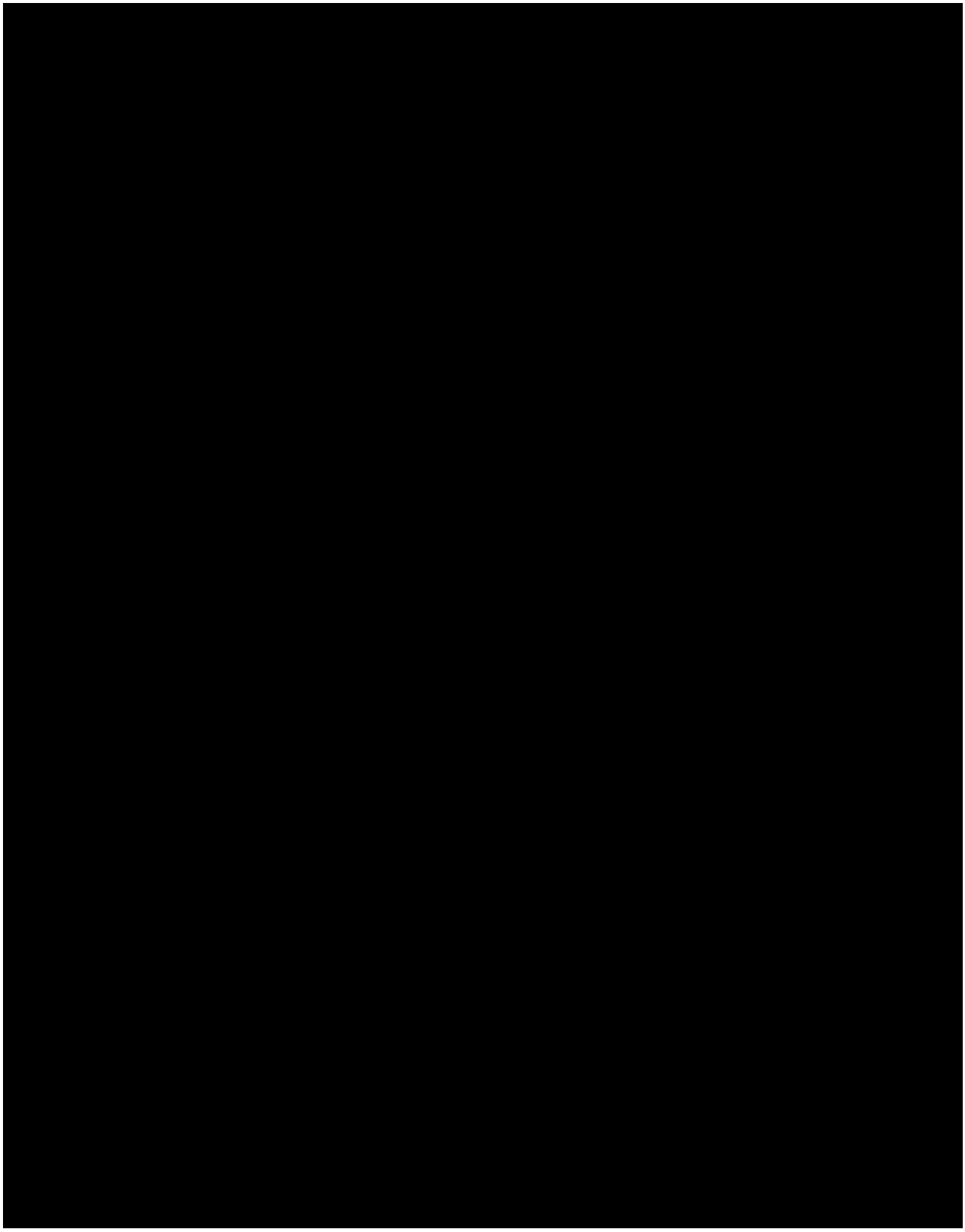
Sicherheitsvorfälle in Quartal 1

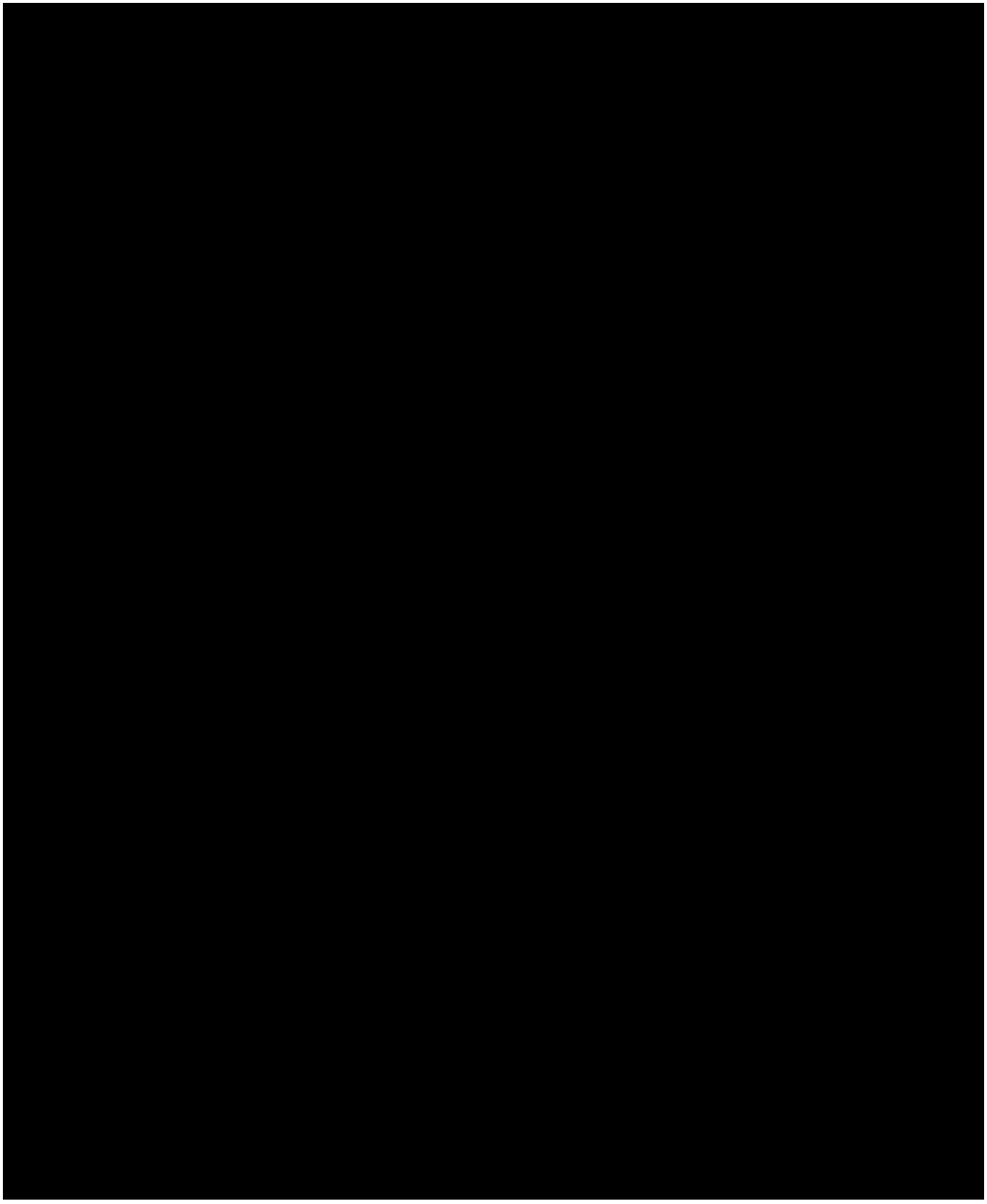
[redacted]

[redacted]

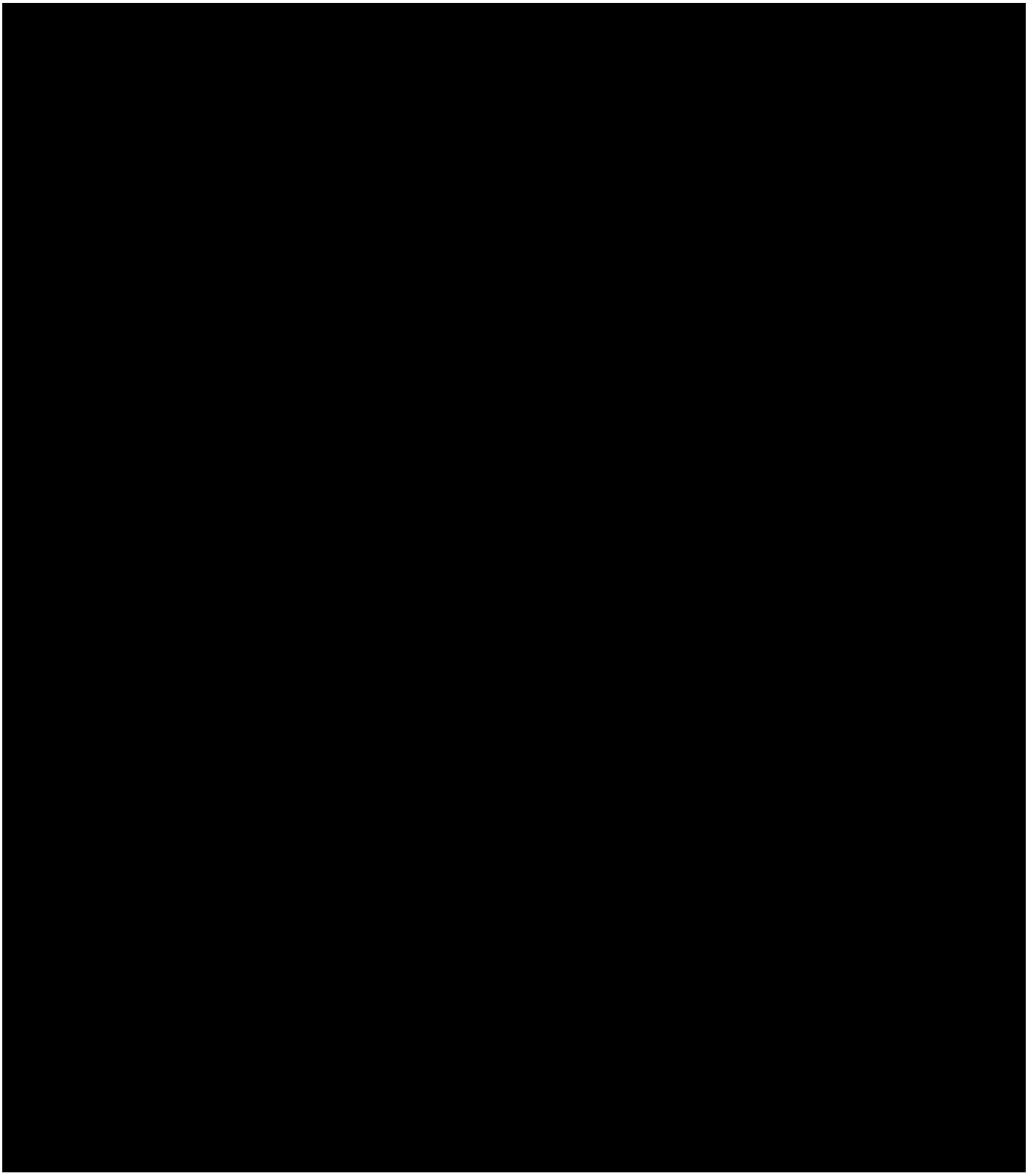
Sicherheitsvorfälle in Quartal 2

[redacted]

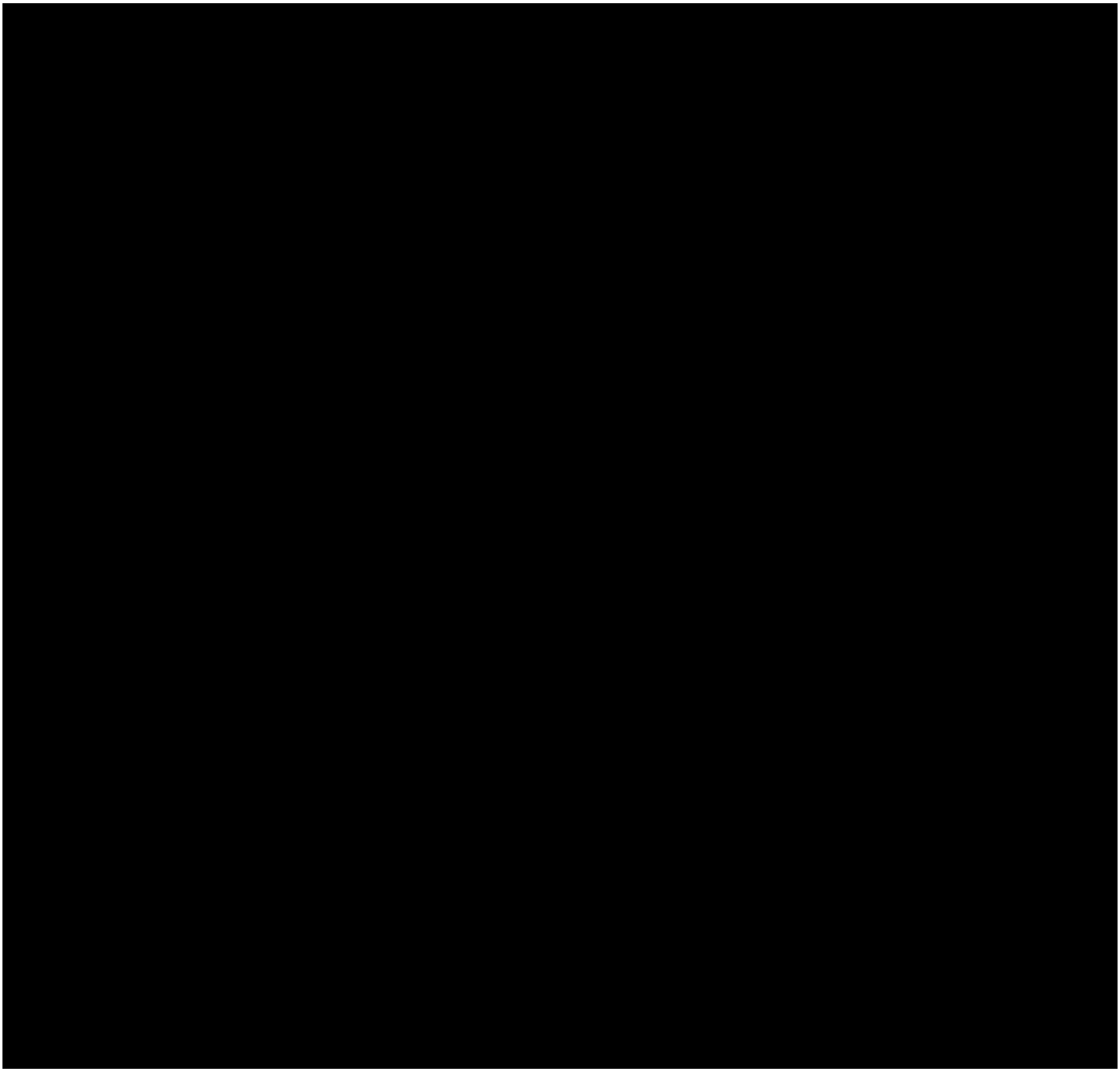




Sicherheitsvorfälle in Quartal 3



[redacted]



Sicherheitsvorfälle in Quartal 4

[redacted]

[redacted]

[redacted]

Weitere Vorfälle

Alle relevanten Schwachstellenfunde und Vorfälle aufzulisten und detailliert zu erläutern, würde den Rahmen dieses Berichts sprengen.

[redacted]

[redacted] In den gemeldeten Fällen wurde weiterer Schaden dadurch abgewendet, dass die Anwender entsprechend sensibilisiert waren, die E-Mails als verdächtig gemeldet und nicht auf den Anhang geklickt hatten. Das CERT NRW geht von einer signifikanten Dunkelziffer nicht erkannter und nicht gemeldeter E-Mails mit Schadsoftware aus. Die Urheber von Schadsoftware modifizieren neue Varianten seit geraumer Zeit da-

hingehend, dass sie zum Zeitpunkt des Versands von keinem der üblichen Antivirusprodukte erkannt werden.

Schulungsangebote und Sensibilisierungsmaßnahmen

Das CERT NRW hat in 2012 verstärkt beratend und sensibilisierend, insbesondere im Bereich der Websicherheit oder anlassbezogen aufgrund von Schwachstellenfunden, mitgewirkt. Dies hat bereits zu einem besseren Bewusstsein für Sicherheitsprobleme auf Seiten zahlreicher Kunden von IT.NRW sowie auf Seiten einiger externer Dienstleistungsunternehmen im Bereich Webentwicklung geführt.
Im Rahmen des IT-Fortbildungsprogramms hat das CERT NRW Informationsveranstaltungen in 2012 angeboten. Zusammen mit dem Referat 321 hat das CERT NRW eine Sicherheitsschulung für Programmierer organisiert, in der neben der Standardabsicherung von Quellcode auch wichtige Punkte wie der Umgang mit Kreditkarten geschult wurden. Für 2013 ist ein Schulungsangebot in Vorbereitung, welches die Vermeidung der wichtigsten bzw. kritischsten Webschwachstellen zum Inhalt hat (OWASP Top 10).

In 2012 wurden die Mitarbeiter des CERT NRW in folgenden Themen extern geschult:

- Computer Security Incident Handling (Vorfallsbehandlung)
- Hacking / Angriffsmethoden
- Webapplication Security
- IT-Forensik (produktspezifisch)

In 2013 sind weitere Qualifizierungs- und Trainingsmaßnahmen erforderlich, insbesondere in den Bereichen Webapplication Security und in der Aufklärung von IT-Sicherheitsvorfällen (IT-Forensik). Für den effektiven Austausch von Warnmeldungen und sicherheitsrelevanten Informationen mit anderen Verwaltungs-CERTs sind Kommunikationsübungen[1] nötig.

[1] Im Januar 2013 hat das CERT-Bund zu diesem Zweck bereits einen Workshop veranstaltet, an dem zwei Mitarbeiter des CERT NRW sowie CERT-Mitarbeiter einiger anderer Bundesländer teilgenommen haben. Der Workshop beinhaltete auch eine Kommunikationsübung.

Kooperationsverbünde

CERT-Verbund

Das CERT NRW ist Mitglied im bundesweiten CERT-Verbund, dem CERTs aus Bundes- und Landes-Behörden sowie aus Privatunternehmen angehören.

In 2012 hat das CERT NRW mit je zwei Mitarbeitern an zwei Arbeitstreffen des CERT-Verbunds teilgenommen:

- 19.04.2012 – 20.04.2012 bei VW in Wolfsburg
- 25.10.2012 – 26.10.2012 bei der Telekom AG in Bonn

Ein vorwiegendes Diskussionsthema auf beiden Treffen war die Erkennung und der Umgang mit so genannten Advanced Persistent Threats (APT).
Aktuell sind die wenigsten Organisationen auf solche Bedrohungen vorbereitet. Zudem wird es zunehmend schwieriger, Massenphänomene (z. B. Bankingtrojaner wie Zeus) von APT Angriffen zu unterscheiden, da sich APTs teilweise der gleichen Botnet-Infrastrukturen und Angriffsmethoden bedienen. APTs unterscheiden sich im Wesentlichen dadurch, dass sie gezielt und nachhaltig vorgehen.

Verwaltungs-CERT-Verbund (VCV)

Der geplante Verwaltungs-CERT-Verbund ist aktuell in Vorbereitung.
BSI-Lagezentrum und CERT-Bund haben bereits eine Liste mit Ansprechpartnern zusammengestellt und schickt regelmäßig Lageberichte und Sicherheitswarnungen an den hierfür eingerichteten Mailverteiler.

Um die Zusammenarbeit der Landes-CERTs untereinander und mit dem CERT-Bund vorzubereiten, wurden ein Workshop für neue CERTs sowie ein Workshop für etablierte CERTs durch das CERT-Bund organisiert. Das CERT NRW hat am zweiten Workshop teilgenommen.

Sicherheitstests

Im Jahr 2012 war das CERT NRW an der Vorbereitung, Durchführung und Koordination mehrerer Sicherheitstests beteiligt.

[redacted]

Ausschreibungen

In 2012 war das CERT NRW an der Ausschreibung des Penetrationstests für [redacted] beteiligt und hat eine Ausschreibung für [redacted] vorbereitet, die zum Zeitpunkt der Schriftlegung dieses Berichts veröffentlicht ist.

Maßnahmenkatalog zur Sicherheit von Webanwendungen

Um die Kontrolle der Sicherheit von Webangeboten der Landesverwaltung zukünftig effektiver und effizienter gestalten zu können, hat das CERT NRW im Jahr 2012 einen Maßnahmenkatalog erstellt. Der Maßnahmenkatalog umfasst Maßnahmen zur präventiven Identifizierung von Schwachstellen, zur zuverlässigeren Erkennung erfolgreicher Angriffe, und zur nachträglichen Aufklärung erfolgreicher Angriffe. Einige kleinere Maßnahmen zur effizienteren Suche nach Schwachstellen wurden bereits umgesetzt bzw. teilweise umgesetzt. Die übrigen Maßnahmen werden zurzeit noch innerhalb von IT.NRW abgestimmt.

Bedrohungslage

Schadsoftware

Schadsoftware, die sich über das Web und via E-Mail verbreitet, wird häufig nicht von Antivirusprodukten erkannt. Wie bereits oben erläutert, modifizieren die Urheber neue Varianten so lange, bis sie von keinem Antivirusprodukt mehr erkannt werden. Aus diesem Grund hat die Effektivität von Antivirusprodukten auch in 2012 nachgelassen. Es müssen zusätzliche Wege gefunden werden, um Infektionen zu vermeiden oder zumindest zu erkennen.

Darüber hinaus ist verstärkt mit gezielten Angriffen zu rechnen, deren Ziel die Gewinnung sensibler Informationen ist (Spionage).

Die Angreifer bedienen sich in solchen Angriffen unter anderem auch weit verbreiteter Schadsoftware als Grundlage und fügen dieser eigene Komponenten hinzu, die auf das Ziel abgestimmt sind.
Wird die Schadsoftware entdeckt, ist selbst für Experten nicht unmittelbar erkennbar, ob es sich um eine weit verbreitete Schadsoftware handelt, oder um eine gezielte Attacke. Durch voreiliges Löschen und Neuinstallieren infizierter Systeme können gezielte und langfristig angelegte Angriffe und Spionage unbemerkt bleiben.

Daher sollte von jedem infizierten System ein Festplattenabbild gesichert werden, damit eine nachträgliche Aufklärung möglich ist.

Darüber hinaus ist es erforderlich, verstärkt eigene Ressourcen und Kompetenzen im Bereich der Schadsoftwareanalyse innerhalb der Landesverwaltung NRW aufzubauen.

Sensible zentrale Verfahren und Anwendungen

Immer mehr Verfahren, Anwendungen und Datenbanken werden landesweit, länderübergreifend und sogar EU-weit zentralisiert.

[redacted]

Diese Verfahren enthalten personenbezogene und andere sensible Daten und sind naturgemäß exponiert, da sie über das Internet erreichbar sein sollen.

Es ist davon auszugehen, dass diese Verfahren ein attraktives Ziel für verschiedene Interessengruppen darstellen. Ein Verlust der Integrität, Vertraulichkeit oder Verfügbarkeit dieser Systeme bzw. deren Daten hat weitreichende Konsequenzen z. B. politischer und rechtlicher Art sowie in der Außenwirkung (Imageschaden).

An der Entwicklung dieser teils sehr komplexen Verfahren sind in der Regel zahlreiche Firmen und Gremien beteiligt. Sicherheitslücken sind unter diesen Bedingungen sehr wahrscheinlich, weshalb die Überprüfung der Sicherheit sowie eine sehr strenge Qualitätskontrolle von der Planungsphase an in jedem Entwicklungsschritt erforderlich sind.

Die auf viele Organisationen verteilten Aufgaben und die aufwändigen Abstimmungsprozesse in solchen Projekten und Verfahren erschweren eine zeitnahe Behebung von Schwachstellen.

Die Landesverwaltung NRW und IT.NRW laufen als Betreiber dieser Verfahren Gefahr, im Falle einer gravierenden Lücke oder eines Sicherheitsvorfalls die primäre Verantwortung zugeschrieben zu bekommen.

Fazit

Das CERT NRW hat sich in 2012 stark auf das Thema Sicherheit von Webanwendungen konzentriert. Zahlreiche Schwachstellen wurden durch das CERT NRW aufgedeckt und konnten kurzfristig behoben werden. Auf diese Weise hat das CERT NRW maßgeblich zur Prävention potentiell gravierender Sicherheitsvorfälle beigetragen. Dies war nur durch das außergewöhnliche Engagement aller beteiligten Personen möglich.

Die oben erwähnten länderübergreifenden Verfahren und die neue Qualität der Bedrohungslage (APT) erfordern eine stärkere Vernetzung auf Länder- und Bundesebene, wie sie mit dem in Planung befindlichen Verwaltungs-CERT-Verbund vorgesehen ist.

Diese stärkere Vernetzung bringt zusätzliche Aufgaben mit sich wie

- häufigere Übungen und Arbeitstreffen mit anderen CERTs
- Ausarbeitung abgestimmter Prozesse
- Einigung auf eine gemeinsame Terminologie, Klassifizierung und Taxonomie

Mit dem Aufbau des Verwaltungs-CERT-Verbunds besteht allerdings die große Chance für die Landesverwaltung NRW und alle anderen Landesverwaltungen, sich den Herausforderungen der Cyber-Bedrohungen gemeinsam erfolgreich zu stellen.