Bochum, den 13. April 2016

Protokoll

der 35. Sitzung des Ärztlichen Beirates

am Mittwoch, den 13. April 2016

während des 1. Interoperabilitätstag

in Bochum

Vorsitz:	Dr. Dr. Hans-Jürgen Bickmann
Gast:	Matthias Redders (Ministerium für Gesundheit, Emanzipation, Pflege und Alter)
	René Salamon Bundesamt für Sicherheit in der Informationstechnik (BSI)
Anwesend:	s. Teilnehmerliste
Beginn:	15.00 Uhr
Ende:	17.00 Uhr

Hinweis: Aus Gründen der besseren Lesbarkeit wird in diesem Protokoll auf eine geschlechterdifferenzierte Formulierung verzichtet. Es wird ausdrücklich darauf hingewiesen, dass Begriffe wie Arzt, Patient, Mitglied usw. immer auch für die weibliche Form stehen, es sei denn, es wird ausdrücklich auf die männliche oder weibliche Form hingewiesen.

TOP 1 Begrüßung

Herr Dr. Dr. Bickmann begrüßt die Anwesenden (s. Teilnehmerliste).

Schwerpunktthemen der Sitzung sind ein Vortrag von Herrn Salamon (BSI) zu dem Thema „Die medizinische Versorgung als kritische Infrastruktur“ und der aktuelle Projektstand in dem Projekt der gematik zum Aufbau der Telematikinfrastruktur. Im Anschluss zur Sitzung des Ärztlichen Beirates findet eine VIP-Tour für die Mitglieder des Ärztlichen Beirats über den IHE-Connectathon statt, der ansonsten unter Ausschluss der Öffentlichkeit stattfindet.

TOP 2 Genehmigung des Protokolls der Sitzung vom 17. Februar 2016

Herr Dr. Dr. Bickmann ruft als nächsten Tagesordnungspunkt die Genehmigung des Protokolls der letzten Sitzung auf. Da keine schriftlichen Einsprüche vorliegen und auch in der

Sitzung keine Beanstandungen angemeldet werden, wird das Protokoll einstimmig ohne Enthaltungen angenommen.

TOP 3 Die medizinische Versorgung als Kritische Infrastruktur: IT - Bedrohungslagen & Aktivitäten des BSI

Herr Salamon (Sektorbetreuer Gesundheit beim BSI) bedankt sich für die Einladung zur Teilnahme an der Sitzung des ärztlichen Beirats und die eingeräumte Möglichkeit über das Thema zu referieren.

In dem Bereich Gesundheit gibt es aus Sicht des BSI (Bundesamt für Sicherheit in der Informationstechnik) drei Sektoren. Die Gesundheitsversorgung, die Labore und die Arzneimittel / Impfstoffe. Für jeden Sektor gibt es im BSI Mitarbeiter, die für diese Bereiche zuständig sind. Im Fokus des Vortrages steht der Bereich der Gesundheitsversorgung.

Zum Einstieg des Vortrages gibt Herr Salamon einen Überblick zu der Entwicklung von Verwaltungen. In der Vergangenheit wurde z. B. in Arztpraxen rein papierbasiert gearbeitet. Im Laufe der Zeit hat der PC Einzug in die Praxen gefunden. Hier wurden mehrere Rechner mit einander vernetzt. So wurden langsam auch im Kerngeschäft die Prozesse und die Geräte miteinander vernetzt. Zu einem späteren Zeitpunkt wurde die Verbindung mit dem Internet aufgebaut. Somit wurden auch Geräte, mit den das Kerngeschäft erledigt wurde, an das Internet angeschlossen. Das Dilemma aus Sicht des BSI ist, dass Geräte des Kerngeschäftes kaum oder nur wenige Schutzmechanismen haben und somit ggf. Angriffen aus dem Internet ausgeliefert sind. Dadurch entsteht ein Bedrohungspotential im Kerngeschäftsbereich für eine Praxis.

Mögliches Angriffsziel kann zum Beispiel der Zugriff auf die Daten des Patienten oder der Angestellten sein, was zu dem Verlust des Vertrauens der Bürger führen kann, denn die Privatsphäre wird verletzt. Weitere Ziele können die Mess- und Laborsystem und die Unterstützungs- und Erhaltungssysteme sein. Das kann ebenfalls Einfluss auf das Vertrauen der Patienten haben und ggf. auch auf die Gesundheit und das Leben. Es gibt derzeit keine Erkenntnisse über den Erfolg eines solchen Zugriffs auf Daten einer Praxis.

Folgende Schwachstellen und Angriffsmittel sind bekannt:

- direkter Zugriffsversuch
- Trojaner / Viren
- Phising

Diese Schwachstellen können aufgrund von technischer / organisatorischer Unzulänglichkeit, aus Unerfahrenheit, Bequemlichkeit und Vertrauensseligkeit entstehen und bieten deshalb Möglichkeiten in eine Infrastruktur technisch von extern einzudringen. Hier spielt der Faktor Mensch eine große Rolle.

Aus aktuellem Anlass geht Herr Salamon auf die Bedrohungslage durch Ransomware in Krankenhäuser ein. Solche Angriffe auf Unternehmen und Institutionen erfolgen täglich. Das sind demnach keine einmaligen Aktionen, sondern gelebter Alltag für Unternehmen und auch Krankenhäuser. Der mediale Hype hat das Thema in die Aktualität gebracht.

Das BSI hat eine Umfrage zum Thema Ransomware in Krankenhäuser durchgeführt, welche nicht repräsentativ ist. Es wurden 88 Krankenhäuser befragt. Von 11% der Krankenhäuser kam die Rückmeldung, dass es keine Auffälligkeiten gibt, bzw. keine Auffälligkeiten bemerkt wurden. In 40 % der befragten Häuser hat es eine erfolgreiche Infektion der Systeme und eine Verschlüsselung der Daten gegeben. 49 % der Krankenhäuser haben die Angriffe und Infektionen erfolgreich abgewehrt. Festzuhalten ist, dass Krankenhäuser derzeit nicht gezielt angegriffen werden, sondern dass es Alltag für Unternehmen und somit auch für Krankenhäuser ist, solche Angriffe abzuwehren. So die Einschätzung des BSI.

Die Krankenhäuser, welche infiziert wurden, konnten zum größten Teil nach 24 Stunden ihre Daten wiederherstellen. Das setzt allerdings voraus, dass eine regelmäßige, tagesaktuelle Datensicherung durchgeführt wird und die Benutzerrechte so eingerichtet sind, dass der Mitarbeiter keine Administrationsrechte besitzt. Denn je mehr Recht der Benutzer hat und einen schädlichen Dateianhang öffnet, um so größer ist auch der möglich auftretende Schaden. Eine professionelle IT ist hier wünschenswert, die ein Rollen- und Rechtekonzept implementiert hat. Ein weiterer Faktor ist das Sichern der Daten. Werden nicht aktuelle Datensicherungen gefahren, so erhöht sich der potentielle Schaden für das Haus und ggf. sind die Daten nicht mehr wiederherzustellen.

Systeme erkennen Infektionen, allerdings nicht zeitnah. Die Virensoftware meldet Infektionen, wenn ihr diese Viren auch bekannt sind. Allerdings werden immer schneller Viren programmiert, so das hier ein zeitlicher Versatz entsteht. Die Menschen erkennen infizierte Systeme oft sehr viel später, indem ihnen auffällt, dass sie auf Daten nicht mehr zugreifen können.

Die Angriffe mit Ransomware leben davon, dass irgendein Benutzer eine Datei öffnet. Dies erfolgt auch häufig. Denn mittlerweile sind die Dateianhänge sehr gut gemacht, so dass der Benutzer im Tagesgeschäft sehr schnell die Datei öffnet und die Schadsoftware im Hintergrund installiert wird und somit die Systeme infiziert. In der Regel werden die Dateien auf den File-Servern verschlüsselt. Es ist derzeit nicht bekannt, ob medizinische Geräte angegriffen wurden. Festzuhalten ist aber, dass bei der Zulassung von medizinischen Geräten der Virenschutz kein Thema ist.

Ein weiterer Aspekt ist, dass Ransomware sich nicht über Würmer verbreitet. Schäden können nicht nur durch Dateianhänge in Emails entstehen, sondern auch durch aufgerufene Web-Seiten im Internet.

Im Vorfeld zur Sitzung sind Herrn Salamon Fragen des Ärztlichen Beirates zugesandt worden, welche nun beantwortet werden.

1. **Wie sind die bekannt gewordenen IT-Angriffe auf Einrichtungen der Verwaltung und vor allem der Krankenhäuser einzuordnen?**
   Wie bereits im Vortrag berichtet, finden diese Angriffe täglich statt. Hier gibt es derzeit keinen Hinweis, dass ein gezielter Angriff auf Krankenhäuser unternommen wurde. Die Programmierer von Ransomware sind darauf aus Geld aus ihrem Handeln zu schlagen und dabei kommt es darauf an möglichst viele Ziele anzugreifen, um entsprechend viel Geld zu bekommen. Frei nach dem Motto, viele Ziele mit kleinen Beträgen, als ein Ziel mit einem hohen Betrag zu erpressen.

2. **Auf welchem Weg ist die Schadsoftware in die Einrichtungen gelangt?**

Durch das Anklicken von Dateianhängen mit infizierten Dateien und teilweise durch den Aufruf von Internetseiten, welche explizit für solche Angriffe programmiert worden sind. Eine Eingrenzung der Schadenshöhe kann durch eine Hardwaretrennung erfolgen. In dem z. B. ausschließlich ein Rechner für Recherchearbeiten genutzt wird und nur dieser Rechner ist mit dem Internet verbunden.

3. **Wie hat sie sich dort verbreitet?**
   Wenn ein Rechner betroffen ist, dann ist es dieser Rechner, bzw. es ist von den Rechten des Benutzers abhängig und von der Vernetzung, wie weit sich eine solche Software ausbreiten kann.

4. **Haben einige der Einrichtungen, die betroffen waren, tatsächlich die geforderte Summe zur Entschlüsselung gezahlt?**
   Ja, es gibt Einrichtungen, die eine Summe gezahlt haben, bzw. mit dem Gedanken spielen eine Summe zuzahlen. Leider kann aber eine Zahlung keine Garantie dafür sein, dass die verschlüsselten Daten vollumfänglich entschlüsselt werden.

5. **Hat dies zur vollständigen Wiederherstellung (Wiederverfügbarkeit) der Daten geführt?**
   Nein, denn in der Regel ist die Datenstruktur zerstört und somit können nicht alle Daten entschlüsselt werden. Sie können logisch nicht mehr gelesen werden. Es geht geht bei den Angriffen ausschließlich um das Geldverdienen und nicht um die Zerstörung der Daten.

6. **Sind die Einrichtungen im Wesentlichen unabhängig von ihrer IT-Strategie betroffen gewesen? Oder gab es spezielle Schwachstellen bzw. mangelnde Sorgfalt die zum Problem geführt haben?**
   Es gibt immer Schwachstellen. Zum einen spielt der Faktor Mensch hier eine Rolle zum anderen gibt es in vielen Fällen keine IT-Strategie in den Unternehmen. Wichtig ist aber, dass das Unternehmen weiß, was es nach einem Befall der Systeme zu tun hat. Hier helfen Störfallbearbeitungskonzepte, in denen die einzelnen Schritte zum Beheben vom potentiellen Schäden niedergeschrieben sind und als Leitfaden dienen können. Aktuelle Netzpläne sind auch sehr hilfreich. Studien zeigen, das Unternehmen erst nach ca. 200 Tagen bemerken, dass etwas innerhalb der Systeme passiert ist.
   Bemerkt wurde auch bei der Schadsoftware, dass es in einigen Fällen eine Schläferfunktion gibt, d. h. sie können nach einem Befall nicht mehr rekonstruieren, wann die Software installiert worden ist und von welchem Rechner.

7. **Welchen Einfluss hat die Sicherungsstrategie des Unternehmens z.B. Cloudsicherung, interne Plattensicherung, decidierte Bandsicherung auf die Wiederherstellbarkeit der Arbeitsfähigkeit gehabt?**
   Eine externe Sicherung ist sinnvoll und hilft bei der Minimierung der Schäden. Eine Spiegelung der Daten reicht dabei nicht aus. Denn diese kann abhängig von den Rechten eines Benutzers durch diesen auch infiziert werden.

8. **Waren vor dem IT-Angriff auch bereits Sicherungskopien betroffen?**
   Bisher gibt es keine Rückmeldungen, ob auch Sicherungskopien von der Infizierung betroffen waren.

9. **Welchen Einfluss hatten Informationsschulungen der Mitarbeiter auf die Beeinträchtigung? Gab es spezielle Schwachstellen bei den IT-Mitarbeitern (z.B. Rechtevergabe, Nutzung des Administrationszuganges für normale Tätigkeiten, wie z. B. eigene Office-Tätigkeiten, Ablage von Daten, Mailnutzung, etc.)?**
   Je mehr Wissen die Mitarbeiter haben und geschult sind, um so sensibler sind diese bei ihrer Arbeit. Wichtig ist dem Mitarbeiter genau die Rechte zu geben, welche er für die Erledigung seiner Aufgaben benötigt. Deshalb sollte es vermieden werden mit Administrationsrechten das Tagesgeschäft abzuarbeiten.

10. **Was kann (konnte) man als Mitarbeiter tun, falls man den Verdacht hatte, dass das eigene Unternehmen betroffen ist?**
    Der Mitarbeiter soll Ruhe bewahren und den Vorfall an der entsprechenden Stelle in seinem Unternehme melden.

11. **Was kann (könnte) man als EDV-Verantwortlicher tun, wenn der Verdacht bestand, dass sich Schadsoftware im Haus befand bzw. schon verbreitet hatte?**
    Maßnahmen ergreifen den Schaden zu minimieren und entsprechende Vorsichtsmaßnahmen ergreifen, wie z. B. Erarbeitung eines Sicherheitskonzeptes, eines Störfallbearbeitungskonzeptes und entsprechende Datensicherungskonzepte und diese dann auch umsetzen.

12. **Was sollte man aus Sicht des BSI tun, um sich als Institution gegen ähnliche zukünftige Angriffe zu wehren?**
    Vorsichtige und kontrollierte Pressearbeit kann den Schaden nach außen minimieren. Eine richtige Krisenkommunikation unterstützt dabei. Hilfreich ist es auch Sicherheitskonzepte zu erstellen und ggf. die Anbindung von mobile Datenträger (USB-Stick) an einem Praxis-PC zu unterbinden. Nicht jeder Mitarbeiter benötigt mit dem Rechner Zugriff auf das Internet. Das Rechte- und Rollenkonzept kann überprüft und ggf. aktualisiert werden.

13. **Gibt es vergleichbare Möglichkeiten für Praxen?**
    Ja. Die Mitarbeiter in den Praxen können sensibilisiert in dem Umgang mit dem PC werden. Unterstützung kann es auch durch die entsprechenden IT-Dienstleister geben, welche das Praxisnetz betreuen. Sie sollten ihre Kunden beraten.

14. **Gibt es vergleichbare Möglichkeiten für Privathaushalte?**
    Für Privathaushalte gibt es die Möglichkeit einen separaten Rechner für das Internet zu benutzen oder eine Virtual Box des BSI zu nutzen, die einen sicheren Internetbetrieb gewährleistet. Eine gewisse Vorsicht und Skepsis bei Dateianhängen ist auch im privaten Umfeld immer ratsam.

15. **Wann wird es in der Verordnung zum IT-Sicherheitsgesetz Vorgaben für die Einrichtungen des Gesundheitswesens geben?**
    Ende des Jahres 2016 wird es hier Vorgaben geben. Welche kritischen Infrastrukturen im Gesundheitswesen darunterfallen, wird im Einzelnen aber erst durch die Rechtsprechung entschieden werden.

16. **Wären die Risiken nach Einführung der TI anders gewesen?**

Herr Salamon hat derzeit noch zu wenig Kenntnisse über die TI und kann nur sagen, dass es in der Endausbausstufe nur autorisierte Kommunikationskanäle gibt und somit die Möglichkeit des Phishings eingeschränkt wird.

TOP 4 Aktueller Stand: Einführung der Telematikinfrastruktur (ORS 1)

Herr Marquardt (Projektbüro der ARGE eGK/HBA – NRW) berichtet in Vertretung von Herrn Herrmann über den aktuellen Projektstatus zur Einführung der Telematikinfrastruktur (ORS 1).

Herr Marquardt berichtet, dass folgende Komponenten zugelassen wurden:

- PKI (Public Infrastructure)
- Backbone zur Anbindung der Zusatzdienste
- Netzdienste

Die gematik lässt derzeit weitere Komponenten weiter zu. Hier ist ein Projektfortschritt zu erkennen.

In dem Los 2 (Testregion Nordwest) befindet sich der Konnektor im Zulassungstest bei der gematik und in der Zertifizierung beim BSI (Bundesamt für Sicherheit in der Informationstechnik). Ebenfalls in der Zulassung bei der gematik befindet sich auch der Intermediär. Hier werden übergreifende Tests mit den Fachdiensten durchgeführt.

Der Losnehmer CGM hat es geschafft die Parkklinik in Kiel zu bewegen, wieder an der Erprobungsphase teilzunehmen. Dieses Haus hatte zuvor die Teilnahme aufgrund eines Wechsel des KIS-Anbieters abgesagt. Somit nehmen in der Testregion Nordwest 6 Kliniken teil.

Die Anschreiben zur Beantragung von SMC-B Karten wurden bereits versendet und in einigen KV´n liegen derzeit bereits Anträge vor.

In dem Los 1 (Testregion Südost) wurde ein Produktmuster des Konnektors der gematik vorgelegt. Eingereicht wurden, wie im Los 2 auch, mehrere eHealth Kartenterminals, welche sich in den Zulassungstests der gematik befinden. Der Versand der Anschreiben zur Beantragung von SMC-B in der Testregion Südost erfolgt ab Mitte Juni 2016.

Das Antrags- und Freigabeportal für SMC-B und HBA wurde von den Leistungserbringern zur Nutzung für die Erprobung freigegeben und Schulungen wurden bereits durchgeführt. Die Beantragungs- und Ausgabeprozesse für die SMC-B mit Endnutzer wurden in der Produktivumgebung erfolgreich durchlaufen.

Die Termine für die Informationsveranstaltungen zur Wissenschaftlichen Evaluation wurden terminiert.

- 06.07.2016 15:00 – 20:00 in der KVWL, Robert-Schimrigk-Str. 4-6, 44141 Dortmund

- 08.07.2016 15:00 – 20:00 in der Zahnärztekammer Nordrhein, Emanuel-Leutze-Straße 8, 40547 Düsseldorf

Zu den Informationsveranstaltungen in NRW werden auch die Mitglieder und Experten des Ärztlichen Beirates eingeladen. Eine entsprechende Bitte ist an die FAU (Friedrich-Alexander-Universität Erlangen-Nürnberg) weitergereicht worden. In den anderen Bundesländern der Testregion Nordwest sind ebenfalls die Informationsveranstaltungen terminiert.

Teilnehmer an den Informationsveranstaltungen generell sind:

- Leistungserbringer aus den Regionen, in denen die Erprobung des Evaluationsgegenstands stattfindet
- Leistungserbringer aus überregionalen Organisationen in einer vergleichbaren Zusammenstellung (z.B. überregionale Träger, die Standards für Leistungserbringer bzgl. interner Prozesse oder interner IT definieren)
- Vertreter der KVen und KZVen der an der Erprobung teilnehmenden KV-/KZV-Bezirke
- Ärztliche Beiräte nach § 5 Abs. 10 der Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte
- die jeweils zuständigen Landeskrankenhausgesellschaften
- Vertreter der Krankenkassen aus den Regionen, in denen die Erprobung des Evaluationsgegenstands stattfindet, sofern der Evaluationsgegenstand direkte Auswirkungen auf die Prozesse in den regionalen Krankenkassen entfaltet
- Vertreter überregionaler Krankenkassen, sofern der Evaluationsgegenstand direkte Auswirkungen auf die Prozesse in den überregionalen Krankenkassen entfaltet,
- die Leitung des Projekts, in dessen Aufgabengebiet der Evaluationsgegenstand auf Auftraggeber Seite fällt
- Gesellschafter der gematik, welche dazu entsprechende Experten benennen
- die Leitung des Betriebs der TI

TOP 5 Verschiedenes

Zum versendeten Memorandum des Ärztlichen Beirates zum Medikationsplan gab es bereits eine Rückmeldung des Bundesministeriums für Gesundheit. Minister Gröhe bedankt sich für die Bereitschaft zur Unterstützung der Umsetzungsarbeiten zur Einführung des Medikationsplans. Ebenfalls haben sich die Bundesärztekammer und die Kassenärztliche Vereinigung Westfalen-Lippe für das Memorandum bedankt.

Die nächsten Termine:

- Die Vorbesprechung zum übernächsten Ärztlichen Beirat ist am Mittwoch den **11. Mai 2016,** um 20:00 Uhr in der Ärztekammer Nordrhein in Düsseldorf.

- Die nächste Sitzung des Ärztlichen Beirats findet am Mittwoch den **29. Juni 2016,** um 15:00 Uhr in der Ärztekammer Nordrhein in Düsseldorf statt.