THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden,
liebe Geschäftspartner,
Freunde und Bekannte,

auch in diesem Jahr war die SySS GmbH bei der CeBIT und wir haben durch viele spannende Vorträge den Fachbesuchern einen Einblick in unsere Arbeitsweise und die Tiefen der IT-Sicherheit geboten. Damit haben wir schon einen und vielleicht den wichtigsten Teil des diesjährigen Mottos der CeBIT erfüllt.

Kreiert aus den englischen Wörtern *Ability*, *Sustainability* und *Responsibility* war *Datability* das Motto der diesjährigen CeBIT und soll Universen verbinden, wenngleich jeder dieser Begriffe allein Motto einer Messe sein könnte.

Ein Kunstbegriff, der wie viele andere seiner Art die Schwierigkeit in sich birgt, nicht bloßes Kunstwerk zu bleiben, sondern auch Botschaft zu werden.

Die Botschaft? Ein Blick in die Zukunft zeigt Roboy, ein von der Universität Zürich entwickelter humanoider Roboter, ausgestattet mit simulierter Muskulatur und der Möglichkeit zu emotionalen Reaktionen. Er feiert bei der CeBIT seinen ersten Geburtstag. Roboys Bauplan ist Open-Source, wer 200.000 Euro investiert, kann seinen eigenen Roboy bauen. Die Bauteile? Diese sind unter anderem ausgedruckt – mit einem 3D-Drucker.

Mit strahlend blauen Augen blickt er in die Zukunft und erinnert an Automatons. Menschen-puppenähnliche Maschinen, die, damals noch mechanisch durch ein komplexes umfassendes Uhrwerk angetrieben, selbständig Bilder malen oder Texte und Gedichte schreiben. Sind sie gut gemacht, so lassen sie den Betrachter vergessen, dass sie künstlich sind. Auch Roboy sitzt und strahlt und hat die Fähigkeit zu begeistern. Er soll einen Beitrag zur Gehirnforschung liefern.

Big Data ist auch ein viel genutztes Stichwort. Immer umfangreicher, aber auch wichtiger werden die Daten, mit denen wir arbeiten und umgehen müssen. Wichtig dabei ist, dass diese Daten sicher sind – auf ihrem Transportweg, aber auch an ihrem Ablageort.

Wir müssen darauf achten, dass hinter dem Wortkoloss *Datability*, die jeweils für sich selbst essentiellen drei Bildungs-Begriffe nicht verschwinden.

Wir, die SySS GmbH, übernehmen Verantwortung für Ihre Daten und Netze, sind wir mit einem Penetrationstest oder der forensischen Untersuchung Ihrer Daten betraut.

Nach den Erkenntnissen des vergangenen Jahres hinsichtlich des Umgangs mit Daten wird deutlich, dass der verantwortungsvolle und abgesicherte Umgang mit Daten zukunftsbestimmendes Thema ist, dem wir uns bereits seit 15 Jahren mit Erfolg und Erfahrung widmen.

Wir unterstützen Sie gerne dabei, dauerhaft Ihre Daten zu schützen und sind gerne jederzeit Ihr Begleiter, wenn es um Ihre IT-Sicherheit geht.

Herzliche Grüße,
Ihr Sebastian Schreiber

Aktuelle Events

08.04.14	LH[1] IHK Ulm
13.05.14	LH[1] Forum Haus der Architekten, Stuttgart
16.05.14	LH[1] Euroforum Deutschland SE, Düsseldorf
21.05.14	LH[1] Vortrag und Worskhop, World Café 2014

[1] Live Hacking

Detaillierte Informationen zu diesen Veranstaltungen finden Sie auf unserer Homepage www.syss.de.

Aktuelle Schulungen

Windows-Angriffe:
02. - 03.04.14
27. - 28.05.14

Exploits:
09. - 10.04.14

IT-Forensik:
06. - 08.05.14

IT-Security I:
12. - 13.05.14

IT-Security II:
14. - 15.05.14

Incident Response:
20. - 22.05.14

Web-App
03. - 04.06.14

PenTests:
06.06.14

Mobile Device:
24. - 25.06.14

IT-Recht:
27.06.14

Bei Teilnahmewunsch oder Fragen wenden Sie sich bitte an info@syss.de.

Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit, wir werden Sie dann umgehend aus dem Verteiler entfernen.

Impressum:
SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 407856-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Diplom-Inform. Sebastian Schreiber
Verantwortlich für Inhalt: Kim Unger

SySS
THE PENTEST EXPERTS.

Compliance und unverschlüsselte E-Mails

Wie die deutsche Rechtsprechung das IT-Sicherheitsniveau maßgeblich erhöht – von Marcus Bauer

Am 17. Juli 2009 sprach der Bundesgerichtshof ein Urteil bezüglich der Pflichten von Compliance-Officers (BGH-Urteil Az.5 StR 394/08), das in dieser Art großes Aufsehen erregte. Darin legte das Gericht dar, dass die Unterlassung von Datenschutzmaßnahmen mit der Beihilfe zum Betrug beziehungsweise Beihilfe zur Ausnutzung von Schwachstellen seitens Innentäter gleichzusetzen sei. Dieses Urteil wiederum zieht eine Pflicht zum Handeln nach sich und findet Ausdruck in dem Begriff Garantenpflicht. Rechtsanwalt Dr. Christoph Knapp bringt den Kern des Urteils folgendermaßen auf den Punkt und verweist auf einen elementaren Teil dieser Pflicht: „In dem Urteil verweist der BGH darauf, dass der Rechtsabteilung in einem Unternehmen eine besondere Funktion auch bei der Verhinderung von Straftaten aus dem Unternehmen heraus zukomme. Dem Angeklagten wurden in seiner besonderen Verantwortungsposition Obhutspflichten für bestimmte Gefahrenquellen übertragen. Hieraus folge eine Sonderverantwortlichkeit für die Integrität des von ihm übernommenen Verantwortungsbereichs.“[1]

Compliance-Officers und Datenschutzbeauftragte tragen also eine besondere Sorge für den Schutz von Daten, damit niemand sie für kriminelle Aktivitäten jeglicher Art missbrauchen kann. Schludern sie allerdings in ihrer Sorgfalt, so leisten sie Beihilfe für jeden Täter, der etwaige Lücken findet und ausnutzt. Ein BGH-Urteil vom 26.02.2013 (KVZ 57/12)[2] wirft Licht auf eine Praxis, die zwar aus Sicht der IT-Sicherheit als gefährlich angemahnt wird, aber dennoch im Unternehmensalltag gang und gäbe ist, nämlich der unverschlüsselte Versand von E-Mails. In diesem Urteil befand der BGH, dass eine Behörde einem Unternehmen nicht zumuten darf, Informationen, die mitunter unter das Betriebsgeheimnis fallen könnten, unverschlüsselt per E-Mail zu versenden. Daraus ergibt sich für Dr. Jens Bücking, Rechtsanwalt für IT-Recht[3], die folgende Fragestellung: Gehört E-Mail-Verschlüsselung zur Compliance-Pflicht? So schlussfolgert er aus dem BGH-Urteil: „Nun hat auch das höchste deutsche Zivilgericht, der Bundesgerichtshof, in der Gewährleistung der Sicherheit der Kommunikation eine – im Ergebnis damit Compliance-relevante – Sorgfaltspflicht gesehen. Aus dem Urteil dürfte zu folgern sein, dass geschäftliche Interna in der Regel nicht unverschlüsselt per E-Mail versandt werden dürfen, da dem Unternehmen bzw. seinen Verantwortlichen, die solche Daten in Kenntnis des Gefährdungspotenzials ungesichert – beispielsweise über das Internet – verschicken (lassen), der Vorwurf des strafbaren Geheimnisverrats zur Last liegen könnte.“[4] Ferner führt er aus, dass bei Gerichten und Verwaltungsbehörden eine eindeutige Tendenz vorhanden sei, Beweisdaten in beweisfester Form zu verlangen, um die Rechtssicherheit sicherzustellen. „In technischer Hinsicht angemahnt werden insbesondere zeitnahe Backups, revisionssichere Archivierungsprozesse, Firewalls, Filter- und Überwachungssysteme, eine Verschlüsselung jedenfalls bei besonders sensitiven oder sonst geheimhaltungshaltigen Daten sowie eben auch ein Kontinuitätsmanagement, das ein Wiederanlaufen nach Wiederherstellung von System und Daten im Schadensfall gewährleistet. Organisatorisch sind geeignete IT-Unternehmens- und Datenschutzrichtlinien und entsprechende Schulungen der Mitarbeiter erforderlich.“[5]

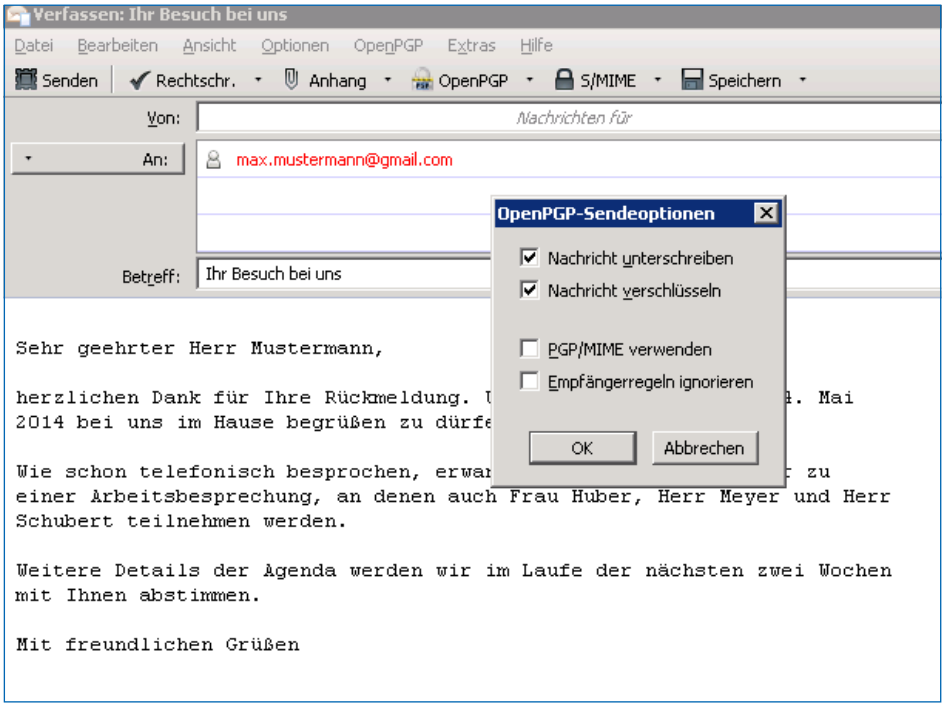
Viele Datenschutzrichtlinien in Unternehmen fordern eine solche Sorgfalt im Umgang mit Daten schon vertraglich. Allerdings hat sich E-Mail-Verschlüsselung im allgemeinen Kommunikationsaustausch noch nicht als Standard etabliert. Nicht immer erfolgt am Anfang einer Kommunikation die Verständigung darüber, wie verschlüsselt kommuniziert werden kann, oder gar der Austausch von Public Keys, wenn beispielsweise PGP im Einsatz ist. Viele, vor allem nicht IT-affine Mitarbeiterinnen und Mitarbeiter in Unternehmen haben wenig Bewusstsein bezüglich der Gefahren, die bei einer Kommunikation in Klartext auftreten können, geschweige denn wissen sie, wie diverse Verschlüsselungsmethoden funktionieren oder wie sie sich beispielsweise einen PGP-Key generieren können. Security Awareness und eine grundsätzliche Aufklärung bezüglich Datenschutz und der gegenwärtigen Rechtslage bei jedem Mitarbeiter im Unternehmen ist daher der erste Schritt für Compliance-Officers und Datenschutzbeauftragte, ihrer Compliance-Pflicht nachzukommen. Weitere Schritte könnte die Etablierung von klaren Prozessen beim Datenaustausch oder die technische Forcierung hin zu verschlüsseltem E-Mail-Verkehr sein.

Die Fragestellung, wie ausschlaggebend die Garantenpflicht ist, wirkt sich für alle Verantwortlichen begünstigend darauf aus, bis dato unbemerkte Lücken und Schlupflöcher zu finden, die ihnen im ungünstigsten Fall bei einem Vorfall auf die Füße fallen könnten. Hier tätig zu werden, ist mit Sicherheit ratsam, denn die Veränderungen in der IT sind stetig. Was heute einen Schutz bietet, mag morgen schon obsolet sein. Zum anderen geschehen kriminelle Vorgänge weitgehend

[1] Siehe http://www.seitz-partner.de/mandanten_pdf/Strafbarkeit%20des%20Compliance%20Officers.pdf
[2] Siehe http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2013&Seite=87&nr=63495&pos=2634&anz=3151
[3] Bücking ist Rechts- und Fachanwalt für IT-Recht, Gründungspartner der Rechtsanwaltskanzle e/s/b Rechtsanwälte, Fachbuchautor im IT-Recht, Lehrbeauftragter an der Hochschule für Technik Stuttgart und IT-Rechtsberater bei Industrie, Handel, öffentlicher Verwaltung und IT-Projekten.
[4] Bücking, Dr. Jens: Compliance-Pflicht E-Mail-Verschlüsselung? In Voi Solutions 1-2014, S. 16
[5] ebd.

leise und oftmals jahrelang unbemerkt, sodass die Lage ein Bild von trügerischer Ruhe und Sicherheit ausstrahlen kann, die eventuell so nicht den Tatsachen entspricht. Dass dieser Bereich den Boden zu illegalen Aktivitäten bietet, zeigt sich in der Art und Weise, wie die Rechtsprechung hierzulande reagiert. So nennt Bücking Beispiele dafür, dass Behörden bezüglich dieser Thematik sensibilisiert sind: „Auch die in zunehmendem Maße versandten Stichprobenerhebungen der Datenschutzaufsichtsbehörden knüpfen in ihrem Fragekatalog folgerichtig bei der Bewertung des Schutzniveaus in Bezug auf die personenbezogenen Daten von Kunden und Mitarbeitern daran an, ob eine E-Mail-Korrespondenz erfolgt. So fragt das Bayerische Landesamt für Datenschutzaufsicht nach den allgemeinen technisch-organisatorischen Maßnahmen zur Sicherstellung der Datensicherheit, nach einem Konzept über die Gesamtheit an Sicherheitsmaßnahmen und – in der Unterrubrik, Einzelpunkte, die in der Praxis oft nicht beachtet werden' – danach, ob E-Mails mit personenbezogenen Daten nur verschlüsselt versendet werden, ob das Unternehmen für die Aufarbeitung einer eventuellen Datenpanne nach § 42 a BDSG vorbereitet ist und ob es dazu einen Notfallplan gibt."[6]

Wie weitreichend Unternehmen ihre Compliance-Pflicht auslegen und an welchen Stellschrauben ihre Compliance Officers und Datenschutzbeauftragte drehen, um ihrer Verantwortung gegenüber Datenschutz in einem legalen Rahmen gerecht zu werden, müssen sie selbst evaluieren. Jedoch ist davon auszugehen, dass dieses Thema auch in der Zukunft aktuell bleiben wird und Datenschutzverantwortliche bei sicherheitskritischen Vorfällen stärker zur Rechenschaft gezogen werden. Daher erscheint es sicherlich sinnvoll, die eigene Compliance besser heute als morgen einer kritischen Überprüfung auf Wirksamkeit und Legalität zu unterziehen und damit zu beginnen, bei der Verschlüsselung von E-Mails PGP und/oder S-Mime als Standard einzuführen.



Screenshot Mail, Quelle: SySS

[6] ebd.