IT-Sicherheitstag Sachsen des „Behörden Spiegel“ gemeinsam mit dem Sächsischen Staatsministerium des Innern am 14. Juni 2018 in Dresden
Fachforum A1: Sensibilisierung von Mitarbeitern

Jochen Hollmann:
„Digitales Bauchgefühl – Der Faktor Mensch in der behördlichen IT-Sicherheit“

Es gilt das gesprochene Wort.

Anrede,
als Leiter der sachsen-anhaltischen Verfassungsschutzbehörde habe ich einen etwas anderen, vielleicht nicht so technischen, Blick auf das große Thema „IT-Sicherheit“. Und doch bin ich mir mit meinen Vorrednern und Ihnen einig über die Bedeutung des Themas.
Auch der Verfassungsschutz kann etwas dazu beitragen, dass IT-Sicherheit angemessene Berücksichtigung findet und was unsere speziellen Beratungs- und Unterstützungsmöglichkeiten im Feld der Mitarbeitersensibilisierung betrifft, das möchte ich Ihnen jetzt gerne vorstellen.

IT-Sicherheit und Digitalisierung

In den 1980er- und 1990er-Jahren gab es nur wenige computergestützte Arbeitsplätze, Automatisierung betraf eher Maschinen und Produktionsprozesse, das Internet war eine eher exotische Spielwiese für verschrobene Sonderlinge in dunklen Kellern meinte als hochkompetente Spezialisten) und Hacking noch eine aufsehenerregende Ausnahme. Heute gibt es das papierlose Büro, vernetzte Arbeitsplätze mit vielen IT-Anwendungen und internetbasierte Kommunikationsstrukturen. Analog der vielbeschworenen „Industrie 4.0“ durchdringen IT-Systeme die Arbeitswelt der Behörden und sind gleichermaßen durch unterschiedlichste Angriffe bedroht. Behörden, Unternehmen, Wissenschaft, Institutionen und Bürger sind heutzutage regelmäßigen Angriffen auf die Integrität, Vertraulichkeit, Verfügbarkeit und die Authentizität ihrer IT-Systeme und der darin gespeicherten Informationen ausgesetzt. Das Eindringen in IT-gestützte Systeme, Manipulation und Sabotage von Systemen, Accounts und Dateien sowie der Diebstahl von Daten sind 2018 reale Bedrohungen.

Es passiert – Akteure und modi operandi

Anrede,
es passiert, jeden Tag und es kann jeden treffen. Hacking, elektronische Angriffe und Datenklau sind Realität in Deutschland. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beispielsweise berichtet in seinen Analysen ebenso regelmäßig wie Fachmagazine für IT und auch die Polizei- und Verfassungsschutzbehörden erfahren regelmäßig von solchen Vorfällen. Wir sehen Angriffe auf die Datenintegrität und auf die Datenverfügbarkeit. Daten werden gefälscht oder verfälscht, um das Handeln öffentlicher Institutionen zu stören oder zu unterbinden.

Es handelt sich um ein Aktionsfeld mit erheblicher Dynamik und hohem Gefahren- und Schadenspotenzial. Seit Jahren steigt die Zahl entsprechender Vorfälle. Angriffsmethoden und –ziele werden ständig variiert und dem technischen Fortschritt folgend ausgeweitet. Ein signifikantes Beispiel war der Angriff auf das Lukaskrankenhaus in Neuss im Jahr 2016 mittels eines Verschlüsselungstrojaners. Der Angriff führte bekanntermaßen zur Einstellung des Krankenhausbetriebs mit allen Konsequenzen.
Es gibt eine Vielzahl von Akteuren und unterschiedliche Angriffsarten und –zielen. Wir als Verfassungsschutz sind dabei grundsätzlich nur dann zuständig, wenn mindestens der Verdacht besteht, dass fremde Nachrichtendienste beteiligt sein könnten. Aber unabhängig davon sehen auch wir das große Ganze und nehmen zur Kenntnis, welche Akteure auf der Bühne agieren.

Es sind vor allem folgende Akteure, die immer wieder auffallen:

- Kriminelle suchen materiell verwertbare Informationen, sie erpressen Geld von ihren Opfern, deren Festplatten verschlüsselt wurden oder denen Straftaten unterstellt werden. Sie manipulieren Informationen, um sich illegal Güter zu verschaffen. Manchmal handeln sie im Interesse einer fremden Regierung, um Stimmungen in der Bevölkerung oder sogar Regierungshandeln zu beeinflussen.
- Sogenannte Hacktivisten verfolgen politische Ziele, indem sie IT-Sabotage oder Datendiebstahl betreiben. Für sie sind gerade behördliche Systeme interessante Ziele.
- Und last but not least suchen fremde Nachrichtendienste vertrauliche Behördeninformationen, um strategische Ziele ihrer Regierungen zu verfolgen oder staatliche Interessen in Bezug auf die Erlangung technischen und wissenschaftlichen Know-Hows durchzusetzen. Elektronische Angriffe gehören zum gängigen Repertoire fremder Nachrichtendienste. Mittels dieser Cyberspionage oder-sabotage wird

versucht, innovative Unternehmen und ihre Geschäftspartner, Forschungseinrichtungen, Universitäten und Behörden zu schädigen oder sich deren Know-how illegal anzueignen.

Anrede,
schaut man sich an, wie Angriffe erfolgen, so finden sich einige typische und beispielhafte Vorgehensweisen:

1. Betrügerische E-Mail-Kommunikation

Elektronische Angriffe werden weit überwiegend mittels E-Mail geführt. Behördenmitarbeiter als Zielpersonen von Angriffen werden vorher ausgespäht. Namen und Kontaktdaten finden sich auf Behördenhomepages, auf Dokumenten als Bearbeiter oder Vorgesetzter oder auch in Präsentationen im Internet. Nicht zu vergessen: Auch Behördenmitarbeiter haben Accounts in Sozialen Medien, wo Angreifer Informationen finden können. Betrügerische E-Mails werden dann in Bezug auf angebliche Absender, Inhalte und Begleitinformationen so gestaltet, dass die Empfänger keinen Verdacht schöpfen. Sie sollen dazu verleitet werden, einen Anhang zu öffnen oder mitgeführte Links anzuklicken. Diese können Schadsoftware enthalten oder auf infizierte Homepages führen, von denen Schadprogramme auf die Systeme zuzugreifen versuchen. Ebenso gibt es E-Mails, die dazu verleiten, persönliche Konten bei Anwendungen, Datenbanken oder Geschäftspartnern samt Kontonamen und Zugangsdaten zu offenbaren.

2. Verschleierte Kontaktanbahnung

Unsere Erfahrungen als Verfassungsschutzbehörde haben gezeigt, dass fremde Nachrichtendienste, insbesondere chinesische Dienste, häufig mit sogenannten Fake-Accounts in Sozialen Medien arbeiten. Als angebliche Wissenschaftler oder Journalisten versuchen sie, Kontakte auch zu Behördenmitarbeitern zu knüpfen, eine Vertrauensbasis zu schaffen und dann an vertrauliche Informationen zu gelangen. Nicht immer legen Sie dabei den nachrichtendienstlichen Hintergrund offen, sondern nutzen durchgängig gefälschte Identitäten zur Informationsgewinnung. Es gibt auch Fälle, in denen es nach Schaffung einer Vertrauensbasis oder aber nach Kompromittierung zu konkreten Anwerbeversuchen fremder Nachrichtendienste kommt.

3. Hacking

Wie ein kürzlich erschienener Medienbericht darlegt, scheinen auch klassische Hackerattacken, die unmittelbar in Zielsysteme eindringen und sich dort fortbewegen, um Datendiebstahl oder –sabotage zu begehen, immer noch erfolgversprechend zu sein.

Der Angriff auf den Deutschen Bundestag im Frühjahr dieses Jahres beispielsweise hat medial große Aufmerksamkeit nach sich gezogen.

4. Gefälschte Webseiten

Schließlich ist festzustellen, dass es Akteuren immer besser gelingt, mittels gefälschter Webseiten widerrechtlich Informationen zu erlangen oder in Systeme einzudringen, sei es mit kriminellem oder nachrichtendienstlichem Hintergrund. Insbesondere Log-In-Portale und Kontozugänge werden täuschend echt gefälscht. Das betrifft sogar betriebs- und behördeninterne Zugangsmöglichkeiten. Hat man Nutzer mit gefälschten Mails mit fingierten Links auf solche Portale gelockt, führt die Eingabe der Nutzerdaten nicht zum erwünschten Log-In, sondern in die Falle. Die gestohlenen Nutzerdaten sind dann der Schlüssel für digitale Einbrüche und Diebstähle. Nutzer bemerken dies möglicherweise nicht, sondern ärgern sich über Fehler beim Anmelden oder beim Kontozugang, die sie nicht auf einen Cyberangriff zurückführen.

Der Faktor Mensch

Anrede,

warum erzähle ich Ihnen das Ganze? Aus der IT-Sicherheitsszene hört man des Öfteren, dass das Problem vor dem Bildschirm säße. Der berühmt-berüchtigte „Faktor Mensch“ eben. Er muss in alle Sicherheitsplanungen einbezogen werden.

Anrede,

„Irren ist menschlich“ sagt der Volksmund. Diese Weisheit machen sich Kriminelle, Hacktivisten, Whistleblower und eben auch fremde Nachrichtendienste zu Nutze. Sie beuten alle menschlichen Eigenschaften aus, die im Büroalltag vorkommen können:

- Neugier,
- Unerfahrenheit,
- Gutherzigkeit,
- Überlastung,
- Leistungsdruck und so weiter.

Mitarbeiter aller Aufgabenbereiche und Hierarchieebenen sind es,

- die mit Schadsoftware behaftete Anhänge aus Versehen öffnen,
- die betrügerische Links anklicken,
- die auf schadenverursachende Webseiten verlinken,
- die auf Betrugsmaschen hereinfallen

- oder ihr Passwort ahnungslos an einen vermeintlichen, täuschend echt nachgemachten „Helpdesk“ weitergeben.

Die Möglichkeiten, Opfer eines Cyberangriffe zu werden, sind vielfältig und oft geht es nicht um Dummheit oder grobe Fahrlässigkeit als Einfallstor für Angriffe. Geschickte Täuschungen und Manipulationen, betrügerische Kontaktanbahnung und dreiste Lügen nutzen viel häufiger Unachtsamkeiten. Sie verstecken sich in der unauffälligen Masse, gaukeln Autorität vor oder bedienen bekannte Erfahrungsmuster in betrügerischer Absicht. Wenn es schnell gehen muss, Drucksituationen bestehen oder aber etwas bekannt – die Gefahr der Routine – oder offensichtlich erscheint, sind die Aufmerksamkeit und die menschliche Vorsicht häufig abgesenkt. Nicht umsonst wird beispielsweise häufig die sogenannte 5-Sekunden-Regel als Sicherheitshinweis zum aufmerksamen und sensiblen Umgang mit E-Mails kommuniziert. Sie enthält einfache Prüfschritte, die das Erkennen möglicher betrügerischer Umstände erleichtern sollen:

1. Kennen Sie den Absender einer E-Mail und stimmt die Mailadresse?
2. Ist der Betreff logisch und schlüssig?
3. Enthält der Mailtext Fehler oder Widersprüche?
4. Ist die Bezeichnung von Links oder Anhängen eindeutig und schlüssig?
5. Haben Sie eine solche Mail erwartet?

Sollte auch eine oder mehrere dieser Fragen mit NEIN beantwortet werden, empfiehlt es sich, die E-Mail zunächst zu ignorieren und den vermeintlichen Absender zu kontaktieren, um die Urheberschaft und das Anliegen zu verifizieren.

Aufmerksamkeit und Vorsicht sind und bleiben die wichtigsten Dinge, um nicht Opfer von IT-Angriffen zu werden. Da wir evolutionär gesehen in Bezug auf IT noch Frischlinge sind, haben wir noch nicht in dem gleichen Maße Instinkte entwickelt, die uns helfen, Gefahren zu erkennen. Diese digitale Arglosigkeit wird von Angreifern ausgenutzt, viel zu oft mit Erfolg. Im wirklichen Leben ist unser Bauchgefühl oft ein guter Ratgeber, im Umgang mit IT muss sich das erst noch entwickeln.

Anrede,

wenn wir über IT-Sicherheit in Behörden und Unternehmen und den „Faktor Mensch“ sprechen, dann gibt es nicht nur Opfer, sondern leider auch Täter. Die sogenannte Innentäterproblematik ist ein Aspekt, der aus meiner Sicht immer noch zu wenig Beachtung findet.

Ich hatte gerade über menschliche Eigenschaften gesprochen, die Angriffe von außen begünstigen. Es gibt aber auch Konstellationen, die die eigenen Mitarbeiter zu Werkzeugen für Andere werden lassen und die in der Behörde Schaden anrichten. Eigenschaften wie

beispielsweise Neid, das Gefühl nicht anerkannt zu sein, Verschuldung, Spielsucht oder Eitelkeit können Ansatzpunkte sein, interne Mitarbeiter für fremde Zwecke zu instrumentalisieren. Das kann dann beispielsweise dazu führen, dass Mitarbeiter sensible Daten oder vertrauliche Informationen an Unbefugte weitergeben oder schützenswertes Know-How abfließt.

Ich habe mich deswegen mit dem vom Meinungsforschungsinstitut Gallup Deutschland veröffentlichten „Engagement Index Deutschland“ beschäftigt. Im Jahr 2016 hatten demnach 15 Prozent aller Mitarbeiter keine emotionale Bindung und 70 Prozent aller Mitarbeiter nur eine geringe emotionale Bindung zu ihrem Arbeitsplatz. Gerade die erstgenannte Gruppe bildet das Personenpotenzial, aus dem sich Innentäter rekrutieren lassen oder die sich quasi selbst „radikalisieren“ und ohne fremde Beeinflussung illoyal werden können. So erklären sich auch die „Durchstechereien“ aus dem Behördenbereich.
Wie bei wirtschaftskriminellen Handlungen wirken dabei die Mechanismen des sogenannten „Fraud-Triangle“. Diese Figur des Betrugs-Dreiecks beschreibt, unter welchen Voraussetzungen Menschen schädliche Handlungen begehen könnten. Eine Antwort auf diese Frage gab bereits vor einem halben Jahrhundert Donald R. Cressey, ein Pionier der Wirtschaftskriminologie:

- Es bedarf zunächst eines Anreizes zur Tat. Die Person könnte z.B. bei Beförderungen übergangen worden sein oder sich sonst wie zurückgesetzt fühlen.
- Sodann muss sich der Person eine günstige Gelegenheit bieten wie beispielsweise der Zugang zu Verschlusssachen oder vertraulichen Dokumenten, Einblicke in heikle Entscheidungen oder Wissen über Schwächen im Internen Kontrollsystem.
- Entscheidend wirkt als Drittes die Fähigkeit der illoyalen Person eine innere Rechtfertigung für das angestrebte Fehlverhalten zu finden, z. B. „Alle machen es.“, „Ich habe eine bessere Behandlung verdient.“

Mitarbeitersensibilisierung

Anrede,
was können wir tun? Gut ausgebildete, motivierte und gesunde Mitarbeiter sind und bleiben das Kapital von Unternehmen und Behörden und sind der beste Schutz vor Angriffen.
Die Erfahrung zeigt, dass Sicherheitsvorgaben, Richtlinien, Dienstvorschriften und –anweisungen sehr wohl zur Kenntnis genommen werden. Wichtige Vorschriften werden nach der Lektüre sogar gegengezeichnet.
Das allein genügt jedoch nicht. Meist liegen die Vorschriften danach in einer Schublade oder einem wenig genutzten Desktopordner des Arbeitsplatz-PCs und ihre Inhalte geraten

langsam in Vergessenheit. Für die aktive Aufmerksamkeit und sichere Instinkte bedarf es dann doch mehr: Informationssicherheit erfordert ein aktives, bewusstes Handeln im Umgang mit der Informationstechnik und ihren oftmals komplexen Abläufen. Die Verbindung von IT und ihren immanenten Risiken muss jedem präsent sein.
Sensibilisierung der Mitarbeiter ist keine einmalige Angelegenheit, sondern muss vertieft und aufgefrischt werden. Schon die alten Römer sagten „repetitio est mater studiorum – Die Wiederholung ist die Mutter der Studien." Regelmäßige Informationskampagnen können bewusste Aufmerksamkeit („Awareness") unterstützen. Risikobezogene Schulungen sind ebenfalls gefordert. So schnelllebig wie die Entwicklung im IT-Bereich ist auch die Entwicklung neuer Angriffsmethoden und -ziele. Veraltetes Wissen schützt nicht vor neuen Gefahren. Gönnen Sie sich und ihren Mitarbeitern regelmäßig Updates, um einen störungsfreien Betrieb Ihrer Behörde dauerhaft zu sichern.
Gleichzeitig hilft eine wertschätzende und sicherheitsbewusste Unternehmenskultur, dass Mitarbeiter nicht zu frustrierten oder verführbaren Innentätern werden.

Anrede,
wichtig ist, dass das Thema IT-Sicherheit nicht in der Schmuddelecke oder im eingangs zitierten „Nerd-Keller" vegetiert. Machen Sie es zur Chefsache und setzen Sie sich aktiv dafür ein. Verhindern Sie, dass der Prophet im eigenen Land nichts gilt. Der IT-Admin und der IT-Sicherheitsbeauftragte, auch oft Behörden-Nerds, so wie wir alle in Routinen verstrickt, von manchen wegen seines Sicherheitsbewusstseins lächerlich gemacht, bedürfen der sichtbaren Anerkennung ihrer Kompetenz und ihrer Aufgaben seitens der Leitungsebene.

Unterstützung durch die Verfassungsschutzbehörde

Anrede,
trotzdem wird es den internen IT-Sicherheitsverantwortlichen manchmal so gehen wie dem Propheten im eigenen Land. Und manchmal bleiben Angriffe auch unbemerkt.

Wir als Verfassungsschutzbehörde möchten mit unserem Wissen, unserer Erfahrung und unserer Expertise gerade die Behörden dabei unterstützen, nicht ins Visier von Angriffen fremder Nachrichtendienste zu geraten. Deswegen gehören Präventions- und Beratungsaufgaben zu unserem Portfolio.

Das betrifft zum einen das Arbeitsfeld „Materieller Geheimschutz". Die Verfassungsschutzbehörde hat Mitwirkungsaufgaben bei der Überprüfung von Personen, die

Umgang mit Verschlusssachen haben sollen oder in Sicherheitsbereichen arbeiten. Darüber hinaus bieten wir auch die Beratung im Umgang mit Verschlusssachen an. Diese Kolleginnen und Kollegen können Sie jederzeit anfragen.

Zum anderen sind wir auch im Bereich der präventiven Spionageabwehr tätig. Mitarbeiterinnen und Mitarbeiter kommen auf Anfrage in ihre Behörde und bieten Informations- und Sensibilisierungsveranstaltungen an. Sie können Lagebilder darstellen oder über neuartige Gefahren oder Angriffskampagnen informieren.
Schließlich suchen wir auch von uns aus den vertraulichen Kontakt zu Behörden, Einrichtungen und Institutionen, wenn uns aus dem Verbund der deutschen Nachrichtendienste Informationen über tatsächliche oder mögliche IT-Angriffe und potentielle Opfer übermittelt werden. Gemeinsam mit den möglicherweise betroffenen Einrichtungen analysieren wir die Lage, beraten zu Gefahrenquellen und Prüfschritten und informieren über Schutz- und Sensibilisierungsmöglichkeiten.

Dazu ein Beispielsfall. Allerdings sehen Sie es mir bitte nach, wenn ich Ihnen diese nur abstrakt schildere, denn viele Details sind vertraulich eingestuft und nur für Berechtigte zugänglich. Das ist übrigens auch ein wichtiger Aspekt unserer Beratungstätigkeit: Vertraulicher Kontakt und vertraulicher Umgang mit sensiblen Informationen – zum Schutz aller Beteiligten.
Bundesweit wurden Hochschulen Ziel eines elektronischen Angriffs, darunter auch eine in Sachsen-Anhalt. Hacker hatten versucht, aus hochschulinternen Netzen im großen Stil dort abgelegte Wissenschaftliche Arbeiten abzugreifen. Man hatte sich mehrere hundert E-Mail-Adressen verschafft und E-Mail-Adressen gezielt angegriffen und Kennworte und Passworte für hochschulinterne Logins geknackt.

Üblicherweise gehen wir in solchen Fällen wie folgt vor:

1. Kontaktaufnahme zum Geheimschutzbeauftragten der Hochschule und Bitte um ein persönliches Gespräch.
2. Erste Sensibilisierung in meiner Behörde und Weitergabe unserer Informationen und mutmaßlich erbeuteter Daten.
3. Die Hochschule soll dann autonom den Hinweisen nachgehen, die Betroffenen ansprechen und zunächst selbst sensibilisieren.
4. Kontakt und Beraten der IT-Verantwortlichen der Hochschule.
5. Erfragen der Ermittlungsergebnisse und Angebot weiterer Unterstützung.
6. Mitarbeitersensibilisierung seitens des Präventionsreferates der Verfassungsschutzbehörde.

Zum Glück ist der elektronische Angriff für die Hochschule in Sachsen-Anhalt glimpflich verlaufen. Die gute und vertrauensvolle Zusammenarbeit war für beide Seiten eine gute und erfolgreiche Erfahrung. Einerseits konnten nachrichtendienstlich wertvolle Erkenntnisse gewonnen werden. Andererseits konnte die Hochschule ihr Wissen um mögliche Cyberangriffe und Verwundbarkeiten erweitern und ihre Mitarbeiter entsprechend sensibilisieren.

Insofern möchte ich Sie ermutigen: Sprechen Sie uns an, nutzen Sie unsere Präventionsangebote. Sie sind kostenfrei, aber sicher nicht umsonst.

Anrede,
IT-Sicherheit und Digitalisierung bergen Chancen und Herausforderungen. Erstere kann man mit Gestaltungswillen und Kreativität fördern. Letzteren sollte man mit Achtsamkeit und Sensibilität begegnen. IT-Sicherheit ist Chefsache und sie sollte Ehrensache aller Mitarbeiterinnen und Mitarbeiter sein. Dies zu fördern, zu unterstützen, Kolleginnen und Kollegen entsprechend zu sensibilisieren und es vorbildhaft selbst zu leben sollte selbstverständlicher Teil der Behördenkultur sein.

In diesem Sinne danke ich Ihnen, dass ich Ihnen vortragen durfte.