ÖFFENTLICHER DIENST

Dr. Thomas Reeg, IT-Sicherheitsmanager bei der Landeshauptstadt München

Trends Der Gesetzgeber hat auf die aktuell sehr dynamische Bedrohungslage reagiert und mit dem IT-Sicherheitsgesetz oder dem Bayerische E-Government-Gesetz entsprechende rechtliche Anforderungen an die Verwaltungen definiert. Somit muss die Sicherheit unserer IT eine zentrale Anforderung im Rahmen unserer Verwaltungs- und Geschäftstätigkeit darstellen.

Skills Neben dem reinen IT-Sicherheits-Know-how macht es Sinn, sich auch in allgemeinen IT-Themen bewegen zu können, um IT-Sicherheitsaspekte integrieren zu können. Natürlich darf man auch die Soft Skills wie Kommunikations-, Teamfähigkeit und analytische Kompetenz nicht außer Acht lassen.

Meine Projekte Ich beschäftige mich mit dem Management, daher ist mein Tag weniger von grün blinkenden Cursorn und miesen Hackerangriffen geprägt, sondern eher von Konzepten und Besprechungen zu Themen wie Risikomanagement, Security Incident Management, Sicherheitsaudits oder allgemeinen IT-Themen wie Prozess- oder Serviceorientierung und ihrem Bezug zur IT-Sicherheit.

Besonderheit Die vielen unterschiedlichen Schutzbedarfe der Informationen der Stadtverwaltung, die Komplexität unserer IT und die sehr unterschiedlichen Tätigkeitsbereiche machen für mich die Arbeit sehr spannend. Und natürlich beschleicht mich dann und wann ein gutes Gefühl, wenn ich darüber nachdenke, dass meine Tätigkeit dazu beiträgt, die Informationsverarbeitung in der Verwaltung für die Menschen in München etwas sicherer zu gestalten.

RECHT IM CYBERSPACE

ITler sorgen in Behörden und Unternehmen für mehr Sicherheit in der virtuellen Welt – worauf es in den unterschiedlichen Bereichen ankommt, verraten Experten aus der Praxis

Text: Eva Ixmeier

ÖFFENTLICHER DIENST

IT-Sicherheits-Mitarbeiter beim Bundeskriminalamt

Skills Interessenten sollten über Kenntnisse aktueller IT-Technologien und spezifische Kenntnisse im Bereich IT-Security, etwa zu aktuellen Gefährdungen für IT-Infrastrukturen, gängige Angriffsmethoden und entsprechende Schutzmaßnahmen verfügen. Bringt ein Bewerber zudem Verhandlungsgeschick und eine klare Ausdrucksweise mit, um komplexe Sachverhalte verständlich und überzeugend darstellen zu können, ist das eine gute Grundlage.

Meine Projekte Ein wesentlicher Bestandteil meiner Arbeit ist die fachliche Beratung. Diese reicht von der Führungsebene des Amtes über den IT-Betrieb bis zum einzelnen Nutzer. Die Beratungsfunktion umfasst unter anderem die Erstellung von Richtlinien und Rahmenvorgaben zur IT-Sicherheit. Natürlich aber auch die Prüfung der Umsetzung von Sicherheitsmaßnahmen im Rahmen von Revisionen und Penetrationstests. Im Zuge von Risikobewertungen werden bestehende Gefahren und Schwachstellen sowie deren Relevanz für ein IT-System betrachtet.

Besonderheit Für den Schutz polizeilicher Daten verantwortlich zu sein und dadurch dazu beitragen zu können, dass das BKA seine gesetzlichen Aufgaben erfüllen kann, ist für mich etwas ganz besonderes. Hinzu kommt ein interessantes Umfeld mit vielfältigen Themen und zahlreichen Projekten – etwa die Einführung von Cloud- und Big Data-Technologien und die verstärkte Nutzung mobiler IT.

PRIVATWIRTSCHAFT

Dr. Kim Nguyen, Fellow der Bundesdruckerei

Herausforderungen Eine der wesentlichen Herausforderungen ist es, organisatorisch und technisch die Sicherheit der eigenen Anwendungen und Daten in der Cloud zu sichern. Darüber hinaus gilt es, möglichen Angreifern einen Schritt voraus zu sein, die eigenen Annahmen immer wieder zu hinterfragen und sich gegen neue Angriffsszenarien zu wappnen.

Skills Bei den sich schnell wandelnden Rahmenbedingungen ist vor allem eines wichtig: der Wille, sich ständig weiterzuentwickeln und Neues zu lernen.

Spannende Projekte Berufseinsteiger können bei allen Projektschritten auf dem Weg zur Digitalisierung mitwirken: Konzeption, Umsetzung, Entwicklung, Betrieb, Weiterentwicklung.

Besonderheit Aufgrund der schnelllebigen Technologien muss man sich immer wieder neuen Herausforderungen stellen. Als Mitarbeiter der Bundesdruckerei gilt es, sich tagtäglich mit IT-Security-Trends zu beschäftigen und auch selbst Trends zu setzen. Denn schließlich ist IT-Sicherheit bei der Bundesdruckerei nicht nur ein Unternehmensbereich, sondern ein zentrales Thema des Produktportfolios.

ÖFFENTLICHER DIENST

Cyberanalyst beim Bundesamt für Verfasssungsschutz (BFV)

Trends Grundsätzlich gibt es gewisse Muster und wiederkehrende Methoden bei Angriffen, zum Beispiel Phishing-E-Mails oder Manipulation von externen Webseiten, über die Schadsoftware eindringen kann.

Meine Projekte Als Cyberanalyst bewerte ich Cyberangriffe von staatlichen Akteuren, die gegen Behörden und die deutsche Wirtschaft gerichtet sind. Ein Beispielprojekt ist der Angriff auf den Bundestag 2015. Im ersten Schritt stellen wir Informationen zusammen: wer könnte der Angreifer sein, welches Interesse könnte dahinter stehen, was können wir in öffentlichen Quellen finden, welche Informationen haben Partner oder andere Behörden. Dann geschehen zwei Schritte parallel: die technische Analyse – eine reine Analyse der Schadsoftware – und die nachrichtendienstliche Analyse, als Alleinstellungsmerkmal des BFV. Anschließend werden alle Informationen be- und ausgewertet. Zum Schluss wird ein Abschlussbericht erstellt und dem Opfer übergeben. Die Arbeit basiert auf drei Säulen: der Prävention von Angriffen, der Detektion, also Erkennung von Angriffen und der Attribution, der Beschreibung des Angriffs.

Skills Kenntnisse im Bereich Schadsoftwareanalyse sind von Vorteil. Nachrichtendienstliche Arbeit kann nicht an der Hochschule erlernt werden, daher gibt es ein großes Schulungsangebot innerhalb des BFV. Bewerber sollten vor allem zwei Dinge mitbringen: analytische und strategische Denkweise gepaart mit sehr großem Interesse am politischen Zeitgeschehen. Enorme Lernbereitschaft und eine gewisse Neugier runden das Bild ab.

Besonderheit Es ist sehr reizvoll, zu wissen, wofür man es tut: für die Gesellschaft. Ich bearbeite sehr spannende Fälle, die sehr nah am zeitgeschichtlichen Geschehen sind.

FREIE WIRTSCAHFT

Nadine Sinner, Research and Project Managerin, Accessec

Aufgabenstellungen In der Automobilbranche gibt es viele verschiedene aktuelle Aufgabenstellungen, zum Beispiel: Authentisierung und Authentifizierung der Steuergeräte untereinander, Forderung nach einheitlichen IT-Sicherheitslevel für die am Netzwerk beteiligten Kommunikationspartner, Sicherheitstechnologien für den Erhalt der Privacy, Einsatz von Zertifikaten für die fahrzeuginterne Kommunikation und die des Fahrzeugs mit der Umwelt sowie die Bewältigung des steigenden Einsatzes von Hardware Security Modules zur sicheren Ablage von Schlüsseln und Zertifikaten

Skills Verständnis von Netzwerktechnik ist eine entscheidende Grundlage. Außerdem sollten Bewerber Durchhaltevermögen, Eigenmotivation, Neugierde und Lernbereitschaft für Themenbereiche auch außerhalb der IT mitbringen.

Spannende Projekte Wir sind mit der Vorbereitung, Betreuung und Forschung in staatlich geförderten Kooperationsprojekten betraut. Hierbei geht es darum, technische Lösungen für zukünftige Fragen der Automobilbranche zu entwickeln und im interdisziplinären Austausch alle Randbedingungen zu berücksichtigen. Im Projekt SeDaFa (Selbstdatenschutz im vernetzten Fahrzeug) bin ich mitverantwortlich für den Aufbau eines Demonstrators des elektrischen Ladens von Fahrzeugen.

Mareike Schmidt, Systemingenieurin im Bereich Cyber Intelligence, ESG

Skills Am wichtigsten ist es, Spaß und Interesse für IT-Security mitzubringen. Da IT-Sicherheit keine isolierte Disziplin ist, ist es notwendig, das Zusammenspiel von unterschiedlichen Technologien zu erkennen und zu verstehen.

Spannende Projekte Bei Projekten in (Cyber-)Intelligence liegt der Fokus nicht nur auf der Abwehr und Aufklärung von Cyber-Angriffen, sondern auch die eigene Informationsgewinnung ist ein wichtiger Bestandteil. Ein aktuelles Projekt beschäftigt sich beispielsweise mit der Entwicklung eines Systems zur explorativen Recherche in Massendaten aus öffentlich zugänglichen Quellen im Internet, der methodengestützten Ableitung verlässlicher Indikatoren und der Unterstützung des Anwenders in der möglichst frühzeitigen Erkennung kritischer Entwicklungen.

Besondherheit Das Besondere ist, dass man für die unterschiedlichen Phasen einer Cyber-Bedrohung neue Lösungen entwickeln oder bestehende Lösungen verbessern kann. Zudem ist es in der IT-Security immer möglich, zwei unterschiedliche Sichtweisen einzunehmen: Die Sicht des Verteidigers und die Sicht des Angreifers.