Knotenpunkt polizeilicher Daten:
Andreas Lezgus in einem Serverraum des LZPD

Foto: Jochen Tack

Angriffe aus dem Netz

»Wir tun alles, um Polizeidaten zu schützen«

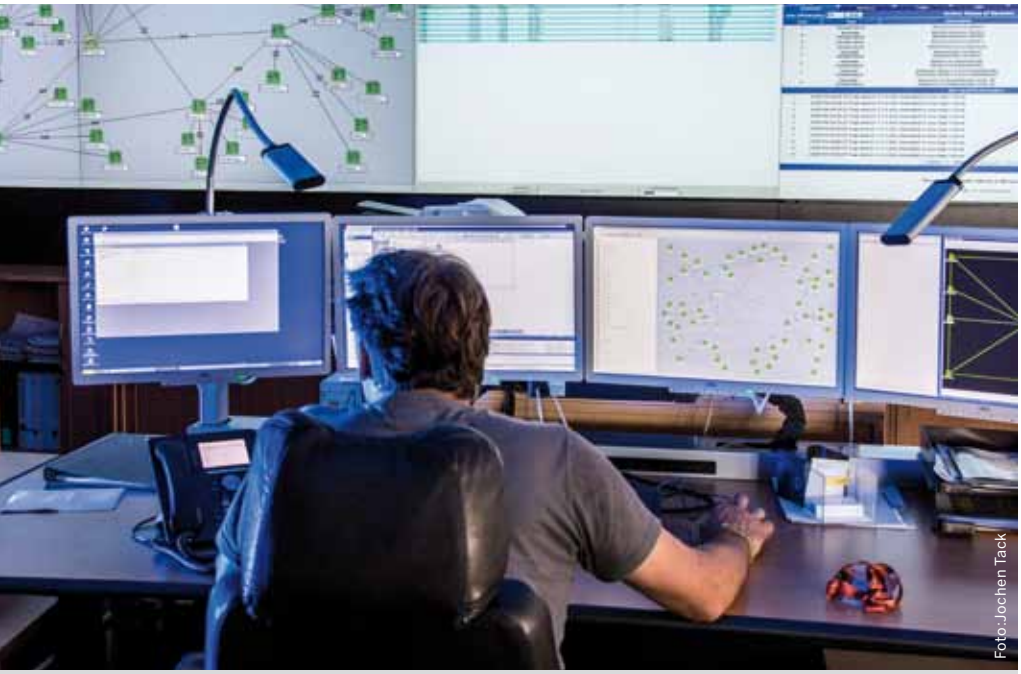
Nicht nur Wirtschaftsunternehmen stehen im Fokus von Cyberkriminellen. Auch öffentliche Einrichtungen und Behörden wie die Polizei sind ein beliebtes Ziel – sie müssen mit täglichen Attacken aus dem Netz rechnen. Die Polizei NRW ergreift daher komplexe Maßnahmen, um die Polizeibehörden und ihre rund 50.000 Mitarbeiterinnen und Mitarbeiter vor Angriffen zu schützen.

Angriffsszenarien gibt es viele: Von sogenannten Distributed-Denial-of-Service-Attacken, zum Beispiel auf einen zentralen Dienst der Polizei, wie etwa den Internetauftritt oder das Bewerberportal bis zu einer Vielzahl an Angriffstechniken auf interne Datenbestände. »Bei diesen DDoS-Angriffen senden Cyberkriminelle gezielt massenhaft Anfragen an unsere Server, so dass der jeweilige Dienst für andere nicht mehr zu erreichen wäre, wenn nicht rechtzeitig darauf reagiert würde«, erklärt der Leitende Polizeidirektor Andreas Lezgus vom Landesamt für Zentrale Polizeiliche Dienste (LZPD) NRW in Duisburg. »Solche Angriffe versuchen wir in der Regel aber frühzeitig zu erkennen und leiten dann die ankommenden Datenströme um, so dass die betroffenen Dienste auch weiterhin erreichbar sind.« Ansonsten sei es hauptsächlich Schadsoftware in E-Mail-Anhängen oder auf Webseiten, mit denen Cyberkriminelle versuchten, Zugriff zu internen Systemen und Datenbeständen zu erlangen. »Diese Art von Angriffen werden durch unsere Sicherheitswerkzeuge gefiltert. Sie prallen quasi schon an der Außenhaut ab«, erklärt Lezgus.

Ein umfangreiches, mehrstufiges Informationssicherheits-Konzept sorgt dafür, dass Cyberkriminelle es möglichst schwer haben, erfolgreich einen Angriff durchzuführen. Grundlage des Konzeptes sind die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), die im »IT-Grundschutz« des BSI festgehalten sind. Darin sind Datenbestände etwa nach bestimmten Kategorisierungen gruppiert: Je kritischer und vertraulicher die zu schützenden Daten sind und je nachdem, wie verfügbar die Daten sein müssen, desto höhere Schutzempfehlungen gibt es. »Wir tun eine Menge, um Polizeidaten zu schützen. Die Polizei arbeitet mit sehr sensiblen Datenbeständen, die einen hohen Schutzbedarf haben, wie etwa Fahndungsdaten, allgemeine polizeiliche Vorgangsdaten oder auch der Austausch mit Staatsanwaltschaften. Daher benötigen wir sehr hohe Sicherheitsstandards, die wir mit unseren verschiedenen Maßnahmenpaketen auch erfüllen«, erklärt der Experte. Die BSI-Maßnahmen beziehen sich zum Beispiel auf die Themen »Gefährdungen«, wie etwa »technisches Versagen«, »menschliche Fehlhandlungen« oder »organisatorische Mängel« sowie unter anderem auf die Bereiche »Infrastruktur«, »Personal«, »Hardware- und Software« oder »Kommunikation«. »Werden alle empfohlenen Maßnahmen des BSI umgesetzt, erreicht man ein hohes Sicherheitsniveau – so auch die Polizei NRW.«

Geprüfter Software-Mix sorgt für Sicherheit

Die Polizei NRW arbeitet mit Produkten verschiedenener Hersteller, etwa von Antivirensoftware, Sicherheitsgateways oder zur Verschlüsselung von Systemen. Interne Sicherheitsbeauftragte prüfen bei Ausschreibungen für diese Produkte, ob die strengen Sicherheitsstandards eingehalten werden. Es wird aber auch eigene Software entwickelt, die neben internen Prüfmaßnahmen zudem von externen Firmen, die auf solche Sicherheitsanalysen spezialisiert sind, getestet wird. Diese Unternehmen führen so genannte Penetrationstests durch, das heißt, sie testen die entwickelte Software auf bereits bekannte, aber auch auf neue Sicherheitslücken. Dabei arbeitet die Polizei unter anderem auch mit Universitäten zusammen, so dass dabei auch die neusten Forschungserkenntnisse einfließen können. Externe Auditoren prüfen außerdem unter anderem die Schnittstellen zu den anderen Polizeien der Länder und des Bundes, um >



Die IT-Leitstelle – Ein 24-Stunden-IT-Service für eine professionelle Polizei

die Sicherheit der Polizeinetzstrukturen zu gewährleisten. »In diesen Audits prüft die Polizei mit wechselnden Sicherheitsexperten, ob und wie die Sicherheitsmaßnahmen des BSI umgesetzt wurden und inwiefern sie bundesweit einheitlich beziehungsweise vergleichbar sind«, so der Leitende Polizeidirektor.

Unterstützung durch CERTs

Als große Behörde benötigt die Polizei NRW auch die Unterstützung der führenden IT-Hersteller und arbeitet eng mit diesen zusammen. Innerhalb der IT-Unternehmen unterstützen die »Computer Emergency Response Teams« (CERTs) Kunden, die spezielle Service- und Wartungsverträge haben und informieren sie frühzeitig über neue Angriffsziele und Sicherheitsprobleme. »Große Organisationen wie wir mit bis zu 40.000 PCs benötigen bei der Beseitigung von Sicherheitslücken ausreichend Vorlaufzeit. Daher erfahren wir von entdeckten Schwachstellen häufig schon vor deren Veröffentlichung, damit wir rechtzeitig entsprechende Gegenmaßnahmen treffen können«, erklärt Lezgus. Dies sei besonders im Hinblick auf so genannte »Zero Day Attacken« wichtig, bei denen Sicherheitslücken bereits am gleichen Tag, an dem sie öffentlich bekannt werden, von Cyberkriminellen ausgenutzt werden. Neben dem Sicherheitsnetzwerk mit den IT-Herstellern ist die Polizei NRW auch mit CERTs aus Bund und Ländern eng vernetzt und tauscht sich über relevante Sicherheitsprobleme aus. »Werden Sicherheitslücken übergreifend eingesetzt, wissen wir das in der Regel ebenfalls ein paar Tage vorher, bevor in den Medien darüber berichtet wird. So können wir gemeinsam abschätzen, welche Auswirkungen eine Schwachstelle auf unsere Systeme haben könnte und welche Vorsichtsmaßnahmen getroffen werden müssen.«

Sicherheit in den Polizeibehörden

Das LZPD ist für die Sicherheit aller zentralen IT-Dienste zuständig, die von allen Polizeibehörden gemeinsam genutzt werden, zum Beispiel für das Rechenzentrum sowie für alle kritischen polizeilichen Verfahren. Für die Netzübergänge zu anderen Behörden sowie das lokale Netzwerk sind die einzelnen Polizeibehörden selbst verantwortlich, das heißt, sie müssen hier den Maßnahmenkatalog des BSI eigenständig umsetzen. Auch hier wird in regelmäßigen Audits geprüft, ob die Behörden sich an die Vorgaben halten. Will eine Behörde ein Verfahren oder eine bestimmte Software »außer der Reihe« einsetzen, muss dafür ein eigenes Sicherheitskonzept zur Genehmigung vorgelegt werden. »Wird das Verfahren genehmigt, ist die Behörde im Anschluss für eine regelmäßige Sicherheitsanalyse verantwortlich und muss sich dazu an festgelegte Sicherheitsleitlinien halten«, erklärt Andreas Lezgus.

Herausforderung Personalentwicklung

Die technischen Fortschritte im Bereich Informationstechnologie sind rasant – und benötigen hochqualifizierte Fachleute, die mit ihrem Wissen stets auf dem aktuellen Stand sind. »Die Polizei kämpft hier mit dem gleichen Problem wie alle öffentlichen Verwaltungen. Wir stehen im Wettbewerb mit den großen Softwareunternehmen, die nicht nur höhere Gehälter zahlen können, sondern auch andere Einstellungskriterien haben«, erklärt der Leitende Polizeidirektor. Um bei der Polizei im IT-Bereich einsteigen zu können, benötigt man in der Regel ein Fach- oder Hochschulstudium. Viele Experten, die im Bereich IT sehr fit sind, haben aber keines. »Die Wirtschaftsunternehmen können regelmäßig besser zahlen und sind in der Einstellungspraxis flexibler – das ist für uns problematisch«, meint der Experte. Dies kann zukünftig dazu führen, dass öffentliche Verwaltungen