Sitzen wir auf einer tickenden digitalen Zeitbombe? Jürgen Neuschwander begrüßt jedenfalls, dass die Bundesregierung Maßnahmen gegen Cyberangriffe unternimmt. BILDER: FOTOLIA / MONTAGE: GORA

ten kriminelle Angreifer sein, die die Stromversorgung gewisser Bereiche ausschalten wollen. Es könnte sich jedoch auch um terroristische Angreifer handeln, die zusätzlich zu physischen Angriffen Chaos verursachen wollen. Die Frage ist: Wer entscheidet jetzt, welche schnelle Eingreiftruppe welcher Behörde nun zum Einsatz kommt? Wer übernimmt die Führung? Diese Fragen sind aus meiner derzeitigen Sicht nicht geklärt. Außerdem wage ich zu bezweifeln, dass sich diese Einheiten immer konsequent untereinander austauschen. Denn möglicherweise möchte jede Behörde seine schnelle Eingreiftruppe gut aussehen lassen und versuchen, das Problem selber zu lösen. Denn das rechtfertigt schließlich auch die Kosten und das Personal dafür.

Wie anfällig ist die öffentliche Infrastruktur in Deutschland denn eigentlich?
Ganz genau kann man das nicht sagen. Sicher ist, dass die Verwundbarkeit in den letzten Jahren kontinuierlich zugenommen hat. Ein Grund ist, dass mittlerweile fast alle Systeme in der öffentlichen Verwaltung massiv mit IT-Technik ausgestattet wurden. Die Administratoren dieser Systeme sind jedoch nicht immer Spezialisten auf dem letzten Stand der Technik. Es fehlt oft das nötige Know-how zum Thema Security. Erschwerend kommt hinzu, dass immer mehr IT-Infrastrukturen untereinander vernetzt werden. Beide Faktoren erhöhen die Anfälligkeit.

Welche Gefahren drohen dadurch?
Gelingt es einem Angreifer, in ein schlecht geschütztes System einzudringen, kann er das System schädigen und er hat durch die eben genannte Vernetzung unter Umständen auch Zugriff auf weitere Systeme. Natürlich gibt es Mittel und Wege um dies zu verhindern – wie zum Beispiel VPN-Verbindungen, die sichere Tunnel aufbauen. Aber auch da gilt, dass es in jedem System Schwachstellen gibt, die gut ausgebildete Hacker durchaus kennen, schlecht ausgebildete Administratoren jedoch nicht.

Gibt es denn überhaupt genügend Fachleute, um den Plan der Bundesregierung umzusetzen?
Nein, momentan gibt es die sicherlich nicht. Aber dieses Problem kann man mittelfristig lösen, indem man mehr Menschen in diesem Bereich ausbildet. Es wird jedoch eine Weile dauern, bis das nötige Know-how aufgebaut wird. Solange muss man sich fähige Leute auf dem Weltmarkt einkaufen.

Einkaufen? Kann sich die Bundesregierung diese guten Leute überhaupt leisten?
Das ist wohl eher eine Frage der Prioritäten. Denn würde sie es nicht tun, und ein Cyberangriff kostet auch Menschenleben, gerät man schnell in Rechtfertigungsnot. Das heißt: Man muss sich diese Spezialisten leisten, um die neuen Strukturen personell auszustatten und den erforderlichen Ausbau voranzutreiben.

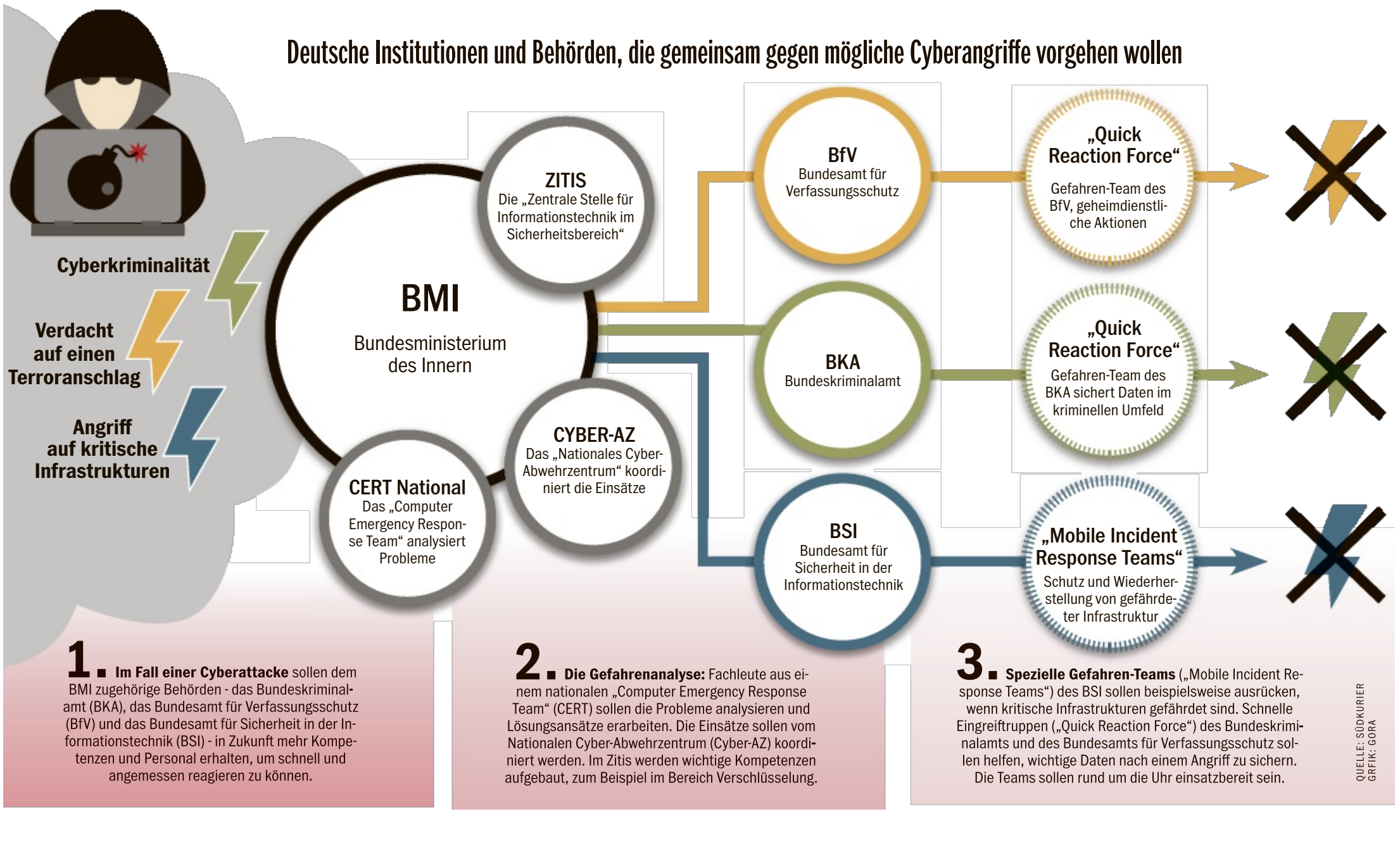
Auch die Bundeswehr treibt die Rekrutierung von Spezialisten voran. Was halten Sie davon?
Ich halte diesen Schritt für vollkommen richtig. Denn potenzielle Gegner werden selbstverständlich versuchen, die Informationswege des Militärs lahmzulegen. Sie werden versuchen, die Kommunikation zu unterbinden, gefälschte Informationen einzustreuen und Netzwerke lahmzulegen. Die Bundeswehr ist seit Jahren bemüht, ihre defensiven Fähigkeiten zur Abwehr solcher Angriffe aufzubauen. Aber vielleicht genügt das nicht. Man muss auch offensive Fähigkeiten entwickeln.

Über die Pläne der Bundesregierung hinaus gedacht: Wo muss die Reise Ihrer Meinung nach hingehen, damit wir besser vor Cyber-Attacken geschützt sind?
Wir müssen im Bereich der IT-Sicherheit wieder autonomer werden. Denn sonst bleiben wir von amerikanischen Software- und Hardware-Herstellern abhängig. Ziel für hochsichere Systeme könnten zum Beispiel eigen entwickelte Hardware-Plattformen sein, die vom BSI abgenommen werden und eben nicht Microsoft- oder Apple-Betriebssystemkerne enthalten. So wüssten wir, woran wir sind. Außerdem sollte man das Thema in der Forschung und in entsprechenden Firmen stärker vorantreiben. Wir haben in diesem Bereich lange nicht investiert. Jetzt müssten wir das massiv intensivieren.

FRAGEN: SUSANNE EBNER

SK PLUS Alle reden über Cyberkriminalität. Aber woher kommt der Begriff „Cyber“ eigentlich? **www.suedkurier.de/plus**

Deutsche Institutionen und Behörden, die gemeinsam gegen mögliche Cyberangriffe vorgehen wollen



1. ■ **Im Fall einer Cyberattacke** sollen dem BMI zugehörige Behörden - das Bundeskriminalamt (BKA), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) - in Zukunft mehr Kompetenzen und Personal erhalten, um schnell und angemessen reagieren zu können.

2. ■ **Die Gefahrenanalyse:** Fachleute aus einem nationalen „Computer Emergency Response Team“ (CERT) sollen die Probleme analysieren und Lösungsansätze erarbeiten. Die Einsätze sollen vom Nationalen Cyber-Abwehrzentrum (Cyber-AZ) koordiniert werden. Im Zitis werden wichtige Kompetenzen aufgebaut, zum Beispiel im Bereich Verschlüsselung.

3. ■ **Spezielle Gefahren-Teams** („Mobile Incident Response Teams“) des BSI sollen beispielsweise ausrücken, wenn kritische Infrastrukturen gefährdet sind. Schnelle Eingreiftruppen („Quick Reaction Force“) des Bundeskriminalamts und des Bundesamts für Verfassungsschutz sollen helfen, wichtige Daten nach einem Angriff zu sichern. Die Teams sollen rund um die Uhr einsatzbereit sein.

QUELLE: SÜDKURIER
GRFIK: GORA