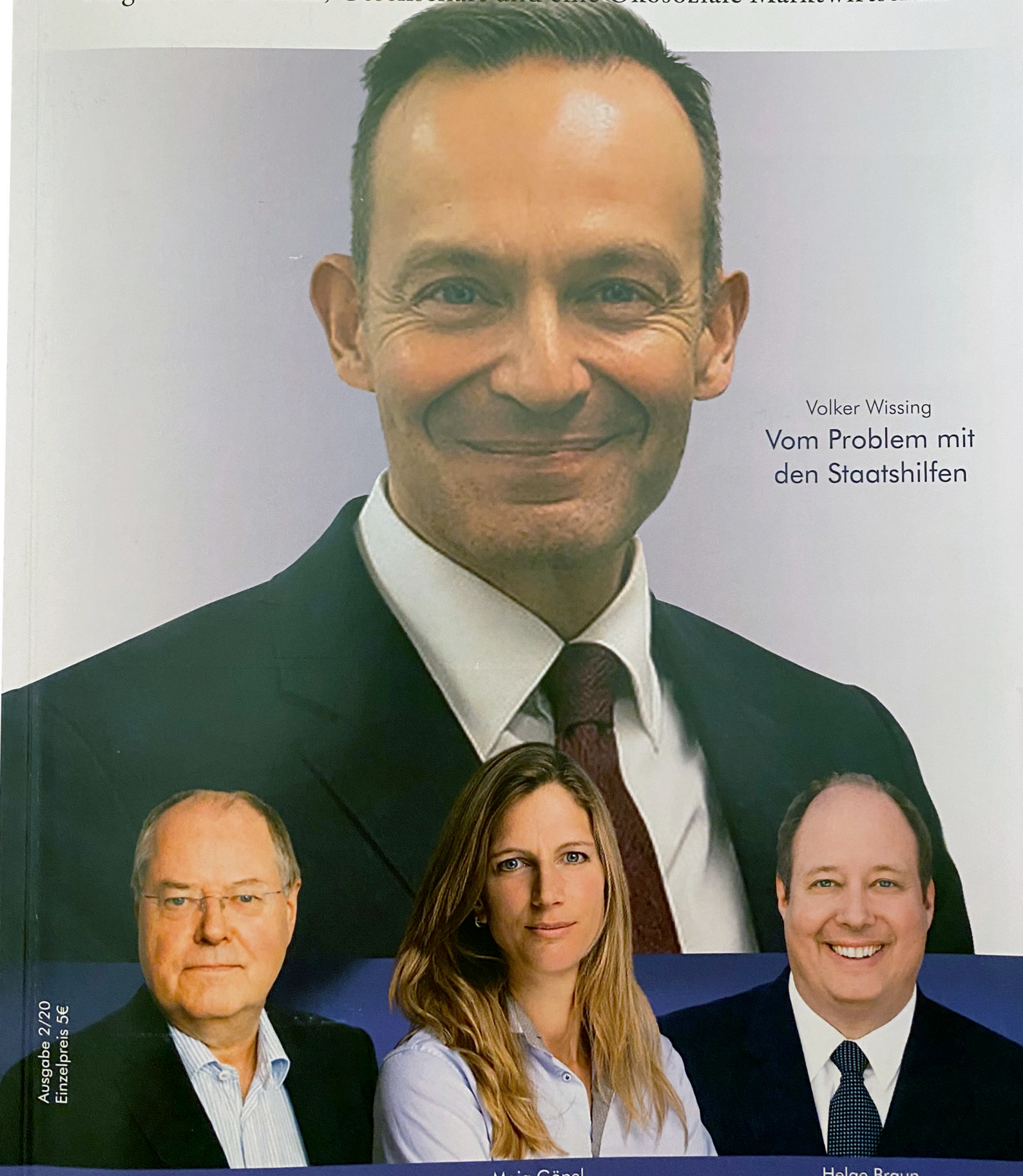
SENATE

Magazin für Politik, Gesellschaft und eine Ökosoziale Marktwirtschaft



Volker Wissing
Vom Problem mit den Staatshilfen

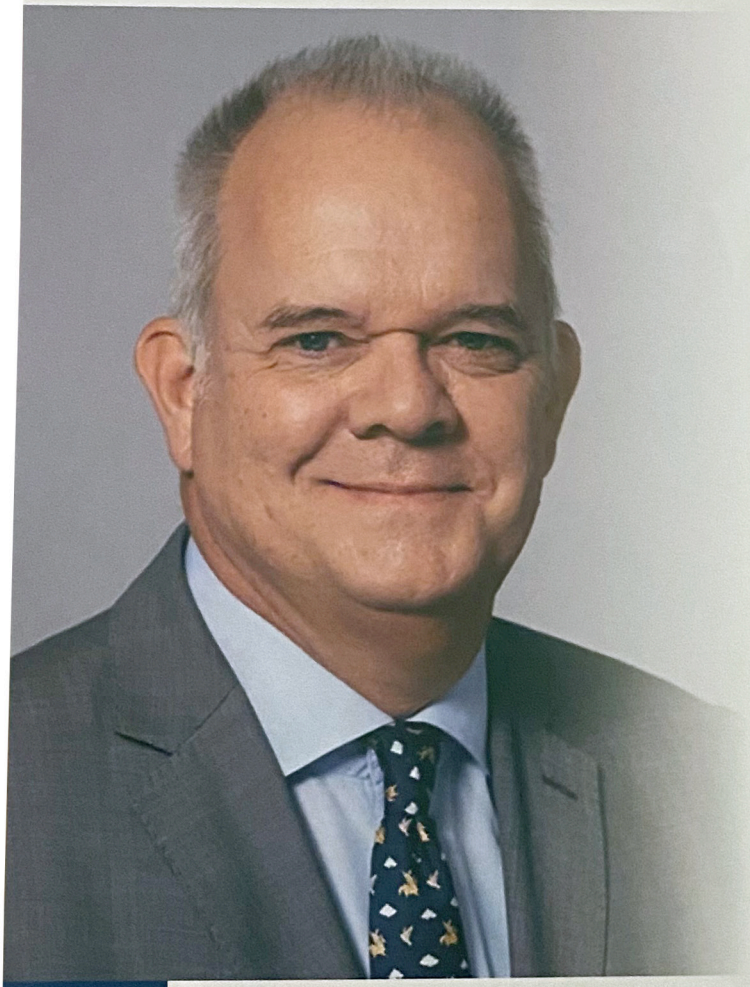
Ausgabe 2/20
Einzelpreis 5€

Peer Steinbrück
Vom Lernen aus der Finanzkrise

Maja Göpel
Vom Neudenken der Welt

Helge Braun
Vom Handeln gegen Corona

Cybercrime im Corona-Modus: digitale Sicherheit auf dem Prüfstand



Stefan Bisanz, Personenschutz-Sachverständiger

Von Stefan Bisanz

Eine Pandemie, wie sie Corona eindeutig ist, ist ein extremes Risiko für die gesamte Menschheit. Pandemien kommen eher selten vor; sie treffen uns allerdings massiv. Um eine Pandemie wie diese bewältigen zu können, sind erhebliche Krisenbewältigungsmaßnahmen notwendig. Nicht nur wegen der Pandemie, sondern auch, weil es Bedrohungen mit der Pandemie gibt. Verstärkt im digitalen Bereich.

Eine Pandemie ist kein Ereignis, welches punktuell wie eine Flut oder ein Tornado kurz und heftig auf uns trifft, sondern eine Krise, die sich lang andauernd in unser Leben schleicht. Maßnahmen, die dagegen beschlossen werden, greifen nicht von heute auf morgen. Auch die jetzige Corona-Pandemie wird noch etliche Monate andauern. Mit der lebensbegleitenden Corona-Pandemie ereilen uns auch einige spezielle Bedrohungsszenarien. Das kann zum einen eine spezielle Anti-Corona-Partei sein, die die Maßnahmen der Regierung zum Schutz der Bürger nutzt, um eigene, oft auch populistische Parolen aufzugreifen und gesellschaftsfähig zu machen. Eine Steigerung sind die so genannten „Corona-Rebellen", die sich insbesondere im Netz sehr stark verbreiten und rechtsextremistisches Sprachgut nutzen, um so die Angst um den Verlust der Bürgerrechte zu kompensieren.

Und Europol sagt einen besorgniserregenden Trend, extremistische Übergriffe für dieses und das nächste Jahr in Zusammenhang mit dem Corona-Lockdown, voraus. Sie vermuten, dass es durch strenge Corona-Maßnahmen vermehrt radikalisierte Einzeltäter geben wird und dadurch die Gefahr von terroristischen Anschlägen steige. Auch die wirtschaftlichen und sozialen Folgen der Corona-Pandemie werden die Radikalisierung steigen lassen.

Es ist immer gut, wenn Unternehmen eine eigene Sicherheitskultur erstellen und leben

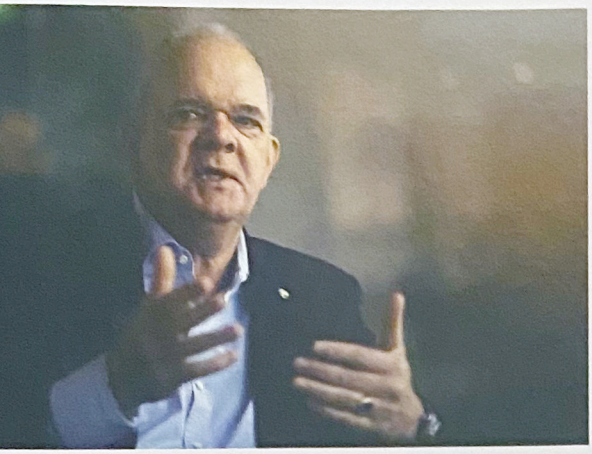
Links- und rechtsextremistische Kreise werden diese Situation nutzen, um ihre Ziele zu propagieren, so Europol. Die Gewaltbereitschaft nimmt zu. Wenden wir uns von diesen Szenarien ab und der Cyber Security zu. Cyber Security war schon vor Corona ein wichtiges Thema, hat aber – durch Einsetzen der Pandemie – erheblich zugenommen und wächst stetig. Cyberattacken nehmen erheblich zu. Warum ist das so?

Einfach formuliert liegt es daran, dass durch die erhebliche Anzahl an Homeoffice-Arbeitsplätzen die Angriffsfläche für Cyberkriminelle rasant gewachsen ist. Inzwischen arbeitet fast jeder Zweite ganz oder teilweise von zu Hause aus. Kleine und mittlere Unternehmen sind nicht in der Lage, ihre Mitarbeiter zu Hause digital zu schützen. Eine ordentliche Digitalisierung, wie sie in dieser Phase viele Unternehmer vorgenommen haben, ist nur mit einer vernünftigen Cybercrime-Strategie möglich. Viele der firmeneigenen IT-Administratoren sitzen nicht im Unternehmen, sondern arbeiten aus dem Homeoffice. Antivirenprogramme gegen gezielte Cyberangriffe sind oftmals nicht am Homeoffice-Platz vorhanden.

Neben dem Digitalisierungsschub, der durch die Homeoffice-Arbeitsplätze entstanden ist, ist es wichtig, dass auch die Informationssicherheit verstärkt werden muss. Da man schnell regieren musste, wurde oftmals ungeprüfte Software angeschafft. Wichtig ist, dass der Beschäftigte im Homeoffice einen sicheren Fernzugriff auf das Datennetz des Arbeitgebers hat. Hier sollte ein sicherer Remote-Zugang geschaffen werden.

Um digital gut aufgestellt zu sein, ist es wichtig, dass man in sichere Systeme investiert. Ein gesamtheitliches Sicherheitskonzept ist ein Wettbewerbs- und Erfolgsfaktor für die vernetzte und digitale Wirtschaft. Diesen Aspekt müssen Unternehmensführer erkennen und umsetzen. Hierzu gehört auch, dass die eigenen Mitarbeiter im Bereich der IT-Sicherheit geschult werden. Es ist immer gut, wenn Unternehmen eine eigene Sicherheitskultur erstellen und leben. Aufgrund der schnellen Verlagerung der Arbeitsplätze vom Firmensitz in die eigenen vier Wände hat sich die Angreifbarkeit von Informations- und Kommunikationssystemen überproportional erhöht. Betriebs- und Geschäftsgeheimnisse müssen auch am Homeoffice-Arbeitsplatz beachtet werden; ebenso alle gesetzlichen Anforderungen im Bereich der Informationssicherheit oder im Datenschutz.

Betrachten wir die Auswirkungen der Corona-Pandemie auf die Cyberbedrohungslage, so stellen wir grundsätzlich drei unterschiedliche Entwicklungen fest. Diese Entwicklung hat die Cybersicherheitslage erheblich verschärft.



1. Durch die unbedachte und plötzliche Entsendung von Mitarbeitern ins Homeoffice gleich zu Beginn der Krise sind Unternehmen für Hacker angreifbarer geworden, da im Homeoffice der Arbeitnehmer sehr oft unsichere IT-Systeme (z.B. die eigenen Laptops der Mitarbeiter) als Arbeitsmittel verwendet. Hacker haben diese Situation ausgenutzt und Mailkampagnen gestartet. Diese Kampagnen hatten das Ziel, den Mitarbeiter im ungesicherten Homeoffice anzugreifen.

2. Seit Ausbruch der Krise ist der gesamte Gesundheitsbereich in den Fokus von Ransomware-Attacken (Verschlüsselung von Daten zur Lösegelderpressung) geraten. Das aktuellste Beispiel ist die Universitätsklinik in Düsseldorf im September. Die Angreifer gehen davon aus, dass aufgrund der Corona-Krise Gesundheitseinrichtungen besonders zahlungswillig sind. Diese Art von Attacken sind im Gesundheitssektor um circa 60 Prozent gestiegen.

3. Hacker nutzen alles, was im Kontext mit Corona steht, um potenzielle Opfer in die Falle zu locken. Themen rund um Corona werden dabei als Köder genutzt. User werden auf gefakte Webseiten im Zusammenhang mit Corona gelockt, da sie dort angreifbarer sind und ihre Daten besser geklaut werden können. In Anhängen zu Mails im Kontext mit Corona wird beim Öffnen oftmals Erpressungssoftware auf den Rechner geladen. Schützen kann man sich durch hohe IT-Sicherheitsstandards.

Um die Sicherheit an dieser Stelle zu gewährleisten und mobiles Arbeiten sicherer zu machen, empfehlen wir folgende Tipps:

1. Awareness-Schulungen der Mitarbeiter
2. Klare Regeln
3. Verstärkte Datensicherung
4. Eindeutige Verifizierung und Identifizierung
5. Verstärkung des Supports für die Mitarbeiter im Homeoffice
6. Vorsicht vor vermehrtem Phishing und Social Engineering
7. Regelmäßige Updates und Monitoring
8. Verschlüsselung der mobilen IT-Systeme und Datenträger

Weiterhin ist es wichtig, sich zum Thema IT- und Cybersicherheit auszutauschen. Effiziente Kommunikation, klare Regeln und Training helfen, sich zu schützen.