Cyber-Kriminalität in Deutschland

(1) Im Mai griff der Software-Virus WannaCry mehr als 230 000 Computer in über 150 Ländern an. Er legte unter anderem Kliniken in Großbritannien lahm, infizierte die Rechner großer Autohersteller wie Nissan und Renault. Innerhalb von vier Tagen richtete WannaCry einen Schaden von mehr als einer Milliarde Euro an.

(2) Was WannaCry im großen Stil praktizierte, erleben viele Firmen täglich im Kleineren. Ihre Computersysteme werden attackiert. Nach Angaben des IT-Verbands Bitcom wurde die Hälfte der Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von Cyber-Angriffen. Schaden: rund 55 Milliarden Euro pro Jahr. Das entspricht fast zwei Prozent des Bruttoinlandsprodukts.

(3) „Das Problem ist, dass die deutschen Unternehmer viel über Cyber-Sicherheit und Gefahren reden, aber verhältnismäßig wenig tun“, kritisiert Hans-Wilhelm Dünn, Generalsekretär des Cyber-Sicherheitsrats Deutschland. **__27__** sehen laut einer Studie des Beratungsunternehmens KPMG 88 Prozent der Führungskräfte deutsche Unternehmen als durch Cyber-Attacken gefährdet an. Aber nur 48 Prozent glauben, dass die eigene Firma bedroht sein könnte.

(4) Dabei sei gerade das oft beschworene „Rückgrat der Wirtschaft“, der deutsche Mittelstand, gefährdet, sagt IT-Experte Dünn. „Die kleinen und mittleren Unternehmen sehen sich selbst oftmals als uninteressant an.“ Doch gerade ausländische Geheimdienste hätten es oft auf deren Know-how abgesehen.

(5) **__29__** in Sachen Cyber-Sicherheit kann Firmenchefs und verantwortlichen Managern teuer zu stehen kommen. „Werden erforderliche Maßnahmen schuldhaft nicht oder nicht hinreichend getroffen“, mahnt der Kölner Anwalt Klaus Brisch, „besteht eine Verantwortlichkeit der Unter-

nehmensleitung, sofern dies zu Schäden für das Unternehmen geführt hat.“ Heißt: Die Firmenleitung muss persönlich für den Schaden haften. Und das kann in die Millionen gehen.

(6) Gerade Mittelständler und Start-ups, die nicht über große IT-Abteilungen verfügen, sollten sich deshalb externen Rat holen. IT-Experte Dünn rät, zunächst die besonders wichtigen Daten des Unternehmens zu identifizieren. „Um diese Kronjuwelen herum kann man dann eine entsprechende Sicherheitsarchitektur errichten, um sie zu schützen“, so Dünn. Außerdem müssten Firmen Notfallpläne für einen Ausfall der Computersysteme erstellen, darin Ansprechpartner festlegen und die Handlungsabläufe üben. Neben Sicherheitsunternehmen bieten auch Behörden Beratung an. Doch Cyber-Security ist kein reines Wirtschaftsthema. Auch das Privatleben wird immer digitaler. So haben laut einer Umfrage des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) 70 Prozent der Internetnutzer mindestens ein Online-Postfach auf einem Kundenportal, 72 Prozent der Bürger aber fürchten sich vor unbefugtem Zugriff auf ihre Daten. Und das Vertrauen, dass sie selbst oder der Staat im Netz wirklich für Sicherheit sorgen können, ist offenkundig gering.

(7) Paradoxe Lage: Laut der DIVSI-Umfrage meinen zwar 83 Prozent der Internet-Nutzer, jeder sei selbst für seine Sicherheit im Netz verantwortlich. Doch 57 Prozent bezweifeln, dass der Einzelne dieser Aufgabe überhaupt gerecht werden kann. 84 Prozent wiederum glauben nicht, der Staat könne dies leisten.

(8) Trotzdem sehen Bürger die Exekutive offenbar in der Pflicht: Vier von fünf Befragten hätten gern eine staatliche Stelle, bei der die Verantwortung für alle Sicherheitsfragen im Internet gebündelt ist. Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), betont, dass seine Behörde die Aufgabe gern übernähme. Der 48-Jährige sieht in der Digitalisierung große Chancen für Staat, Wirtschaft und Bürger. Damit alle von diesen Chancen profitieren können, unterstützt das BSI IT-Anwender durch konkrete, praxisorientierte Angebote, etwa in Form von Informationen und Handlungsempfehlungen.

naar: Focus, 19.08.2017

Tekst 8 Cyber-Kriminalität in Deutschland

1p **26** Wie verhält sich der 1. Absatz zu den nachfolgenden Absätzen?

A Er führt ein internationales Beispiel eines Phänomens heran, das anschließend für die deutsche Situation erörtert wird.
B Er führt einen Extremfall eines Angriffs auf, dessen Verursacher in den nächsten Absätzen besprochen werden.
C Er gibt einen zusammenfassenden Überblick über die nachfolgenden Absätze.
D Er schildert eine überspitzte Gefahr, die anschließend relativiert wird.

1p **27** Welche Ergänzung passt in die Lücke in Zeile 15?

A Also
B Stattdessen
C Tatsächlich
D Trotzdem

1p **28** Welche Funktion hat der 4. Absatz?

A Analyse des Problemausmaßes
B Begründung der KPMG-Studie
C Konkretisierung der Cybercrime-Methoden
D Präzisierung der Risikogruppe

1p **29** Welche Ergänzung passt in die Lücke in Zeile 24?

A Der Egoismus
B Die Offenherzigkeit
C Die Ratlosigkeit
D Die Zurückhaltung

Behalve het verbeteren van de beveiliging zouden bedrijven volgens Dünn nog meer moeten doen (alinea 6).

2p **30** Geef van elk van de volgende zaken aan of bedrijven deze volgens Dünn wel of niet zouden moeten aanpakken volgens deze alinea.

1 kennis met branchegenoten delen
2 efficiënter met kantoorsoftware omgaan
3 calamiteitenprotocol opstellen en handhaven
4 manier van gegevensuitwisseling met klanten heroverwegen

Noteer achter elk nummer op het antwoordblad 'wel' of 'niet'.

„Paradoxe Lage" (Zeile 46)

1p **31** Wieso paradoxal?

A Internetnutzer haben Angst vor unbefugten Zugriffen auf ihre Daten, schützen sich aber überhaupt nicht.
B Internetnutzer halten es für normal, völlig für ihre Daten zu haften, sehen dies aber als eine kaum zu leistende Aufgabe an.
C Internetnutzer sind zwar zuständig für ihre Daten, finden aber, dass der Staat die Daten sicherstellen sollte.
D Internetnutzer vertrauen weder dem Staat noch kommerziellen Kundenportalen, haben aber schon Online-Postfächer.

1p **32** Was kann man aus dem 8. Absatz über Arne Schönbohm schließen?

A Er ist darüber enttäuscht, dass seinem Institut ein staatlicher Auftrag entgangen ist.
B Er ist dazu bereit, den Wünschen der Internetnutzer in Sachen Sicherheit im Netz entgegenzukommen.
C Er sieht ein, dass der Staat die Sicherheit der Internetnutzer nicht garantieren kann.
D Er sieht eine Gefahr darin, dass eine wachsende Anzahl von Unternehmen IT-Sicherheitsberatung im Netz anbietet.