Attribution of a Russian cyber campaign

The Federal Government condemns in the strongest possible terms – and with the support of the European Union, NATO and international partners – the campaign by the state-sponsored cyber actor APT28 that targeted the Executive Committee of the Social Democratic Party of Germany.

The Federal Government's national attribution procedure regarding this campaign has concluded that, for a relatively long period, the cyber actor APT28 used a critical vulnerability in Microsoft Outlook that remained unidentified at the time to compromise numerous email accounts.

Based on reliable information provided by our intelligence services, the actor APT28 has been attributed to the Russian Federation, and more specifically to the Russian military intelligence service GRU.

What is more, this actor's campaign also targeted various government authorities and companies in the spheres of logistics, armaments, the air and space industry, and IT services, as well as foundations and associations. It was directed at entities in Germany, other European countries and targets in Ukraine.

APT28 is also responsible for the cyber attack that was perpetrated on the German Bundestag in 2015.

Such irresponsible actions in cyberspace contravene international cyber norms and deserve special attention, especially in a year in which many countries are holding elections.

Cyber attacks against political parties, state institutions and companies that provide critical infrastructure pose a threat to our democracy, our national security and our liberal-minded society.

The Federal Government most strongly condemns the repeated and unacceptable malicious cyber activities by state-sponsored Russian actors and again calls on Russia to refrain from such behaviour. Germany is determined to work together with its European and international partners to counter such malicious cyber activities.