Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Die Lage in Zahlen

im September 2021

Vorbemerkungen **3**

Zahl des Monats **4**

1 Bedrohungslage **5**

1.1 E-Mails und Spam-Mails in der Wirtschaft in Deutschland 6
1.1.1 E-Mail-Aufkommen in der Wirtschaft in Deutschland im September 2021 6
1.1.2 Spam-Mail-Index für die Wirtschaft in Deutschland im September 2021 7
1.1.3 Spam-Ratio in der Wirtschaft in Deutschland im September 2021 8

1.2 Malware 9
1.2.1 Neue Malware-Varianten insgesamt von Oktober 2020 bis September 2021 9
1.2.2 Neue Windows-Malware-Varianten von Oktober 2020 bis September 2021 10
1.2.3 Neue Malware-Varianten für Anwendungen von Oktober 2020 bis September 2021 11
1.2.4 Neue Malware-Varianten für Android-Geräte von Oktober 2020 bis September 2021 12
1.2.5 Potenziell unerwünschte Anwendungen (PUA) für Windows von Oktober 2020 bis September 2021 13
1.2.6 Potenziell unerwünschte Anwendungen (PUA) für Android von Oktober 2020 bis September 2021 14

2 Schutz der Bundesverwaltung **15**

2.1 Spam-Schutz in der Bundesverwaltung 16
2.1.1 E-Mails an die Bundesverwaltung insgesamt im September 2021 16
2.1.2 Spam-Mail-Index für die Bundesverwaltung im September 2021 17
2.1.3 Spam-Ratio in der Bundesverwaltung im September 2021 18

2.2 Malware-Schutz in der Bundesverwaltung 19
2.2.1 Neue Sperrungen maliziöser Webseiten von Oktober 2020 bis September 2021 19
2.2.2 Index über die Malware-Angriffe auf die Bundesverwaltung von Oktober 2020 bis September 2021 20

Glossar **21**

Quellenverzeichnis **22**

Vorbemerkungen

Erläuterungen

Mit dem Kennzahlenbericht „Die Lage in Zahlen“ legt das BSI eine monatliche Übersicht über die für die aktuelle Lage bedeutsamen Kennzahlen und Entwicklungen vor. Für die Berechnung der Kennzahlen werden Tagesaggregate verwendet. Dabei handelt es sich um die von 00:00 Uhr bis vor 24:00 Uhr aufsummierten Ergebnisse der Einzelerhebungen. In der E-Mail-Verkehrsstatistik sind das also beispielsweise E-Mails je Tag.

Die Tagesaggregate fließen mit spitzen Werten, d.h. mit allen Nachkommastellen, in die Kennzahlenberechnung ein. Es kann daher zu Rundungsdifferenzen kommen. Die Monatsdurchschnitte der Kennzahlen werden zudem als echte Durchschnitte der Tagesaggregate berechnet. Eine Monatsaggregation findet nicht statt.

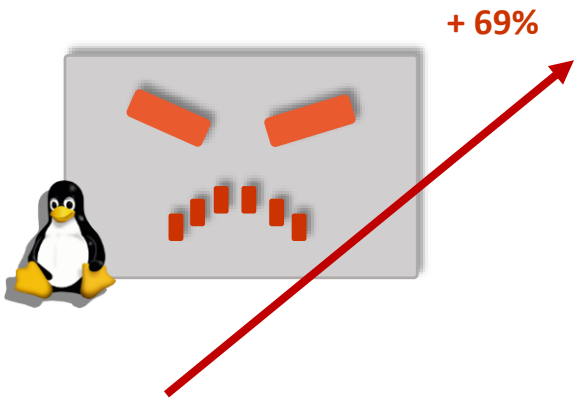
Zeichenerklärung

f	Wert wurde fortgeschrieben.
.	Wert ist unbekannt.
-	Wert ist empirisch Null (d.h. nichts vorhanden).
0	Wert ist rechnerisch Null (d.h. empirisch größer als nichts).
X	Aussage ist nicht sinnvoll.
r	Wert wurde gegenüber früheren Publikationen berichtigt.
/	Wert ist statistisch unsicher und wird daher nicht ausgewiesen

Zahl des Monats

Botnetz XorDDoS sorgt für kräftigen Zuwachs bei Linux-Malware: + 69% gegenüber dem Vormonat

Linux-Malware-Varianten sind üblicherweise so selten, dass sie statistisch nicht auffallen. Im September 2021 war nun mit durchschnittlich täglich 3018 neuen Linux-Malware-Varianten erstmals eine statistisch signifikante Menge zu verzeichnen. Das waren insgesamt mehr als 72.000 neue Linux-Malware-Varianten und ein Produktionszuwachs von 69 Prozent gegenüber dem Vormonat[1].



Verantwortlich für den Anstieg war der Linux-Trojaner XorDDoS, der seit 2014 bekannt ist. Das XorDDoS-Botnetz wurde seinerzeit für großvolumige DDoS-Angriffe genutzt. Es verwendet neben infizierten Linux-Desktop- und –Serversystemen insbesondere auch infizierte IoT-Geräte, die in der Regel mit embedded linux ausgestattet sind.

Bereits seit Mitte 2020 traten wieder vereinzelt neue Varianten auf, die jetzt auch auf offene Docker Server zielen[2]. Im September 2021 war nunmehr mit täglich durchschnittlich 2410 neuen Varianten ein deutlicher Zuwachs zu verzeichnen. Knapp 80 Prozent der neuen Linux-Varianten waren XorDDoS-Varianten. Die gesteigerte Produktivität der Angreifer dürfte darauf zielen, das XorDDoS-Botnetz durch die Infektion weiterer Systeme zu vergrößern und auszubauen.

Die Angreifer hinter XorDDoS verschaffen sich zunächst mit Hilfe eines Brute-Force-Angriffs gegen SSH- und Telnet-Ports Zugang zu einem System. Die integrierte Rootkit-Komponente ermöglicht es ihnen sodann, die Spuren der Malware über mehrere Infektionsstufen hinweg zu verwischen und im System zu verstecken. Ist das System einmal übernommen und dem XorDDoS-Botnetz hinzugefügt, kann es von den Angreifern für DDoS-Angriffe missbraucht werden. Zudem besitzt XorDDoS Backdoor- und Downloader-Funktionalitäten. Angreifer können dementsprechend nicht nur andere Schadsoftware nachladen, sondern sich auch leicht wieder Zugang verschaffen, nachdem das infizierte System (allerdings erfolglos) bereinigt wurde.

[1] Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH. Als Malware-Variante zählt jede im Hinblick auf ihren Hashwert einzigartige Variante einer Malware.

[2] Quelle: https://www.trendmicro.com/en_us/research/20/f/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers.html

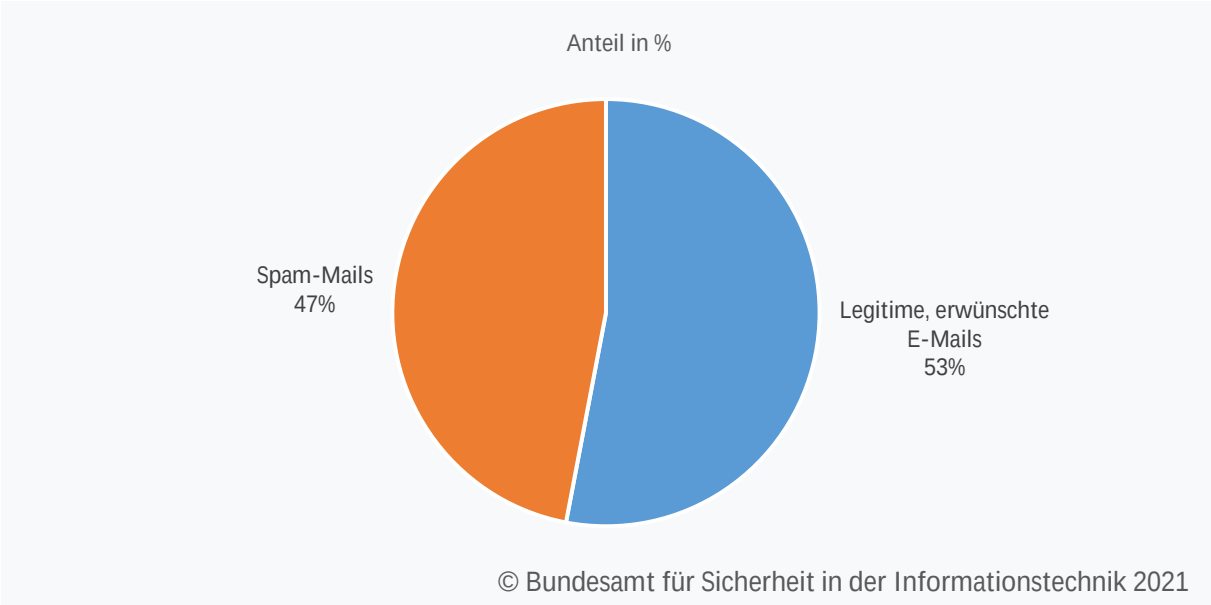
1 Bedrohungslage

1.1 E-Mails und Spam-Mails in der Wirtschaft in Deutschland

1.2 Neue Malware-Varianten und neue PUA-Varianten

1.1 E-Mails und Spam-Mails in der Wirtschaft in Deutschland

1.1.1 E-Mail-Aufkommen in der Wirtschaft in Deutschland im September 2021



Spam-Quote in der Wirtschaft in Deutschland im September 2021 bei 47 Prozent

Sachverhalt

Im September 2021 umfasste der E-Mail-Verkehr in der Wirtschaft in Deutschland durchschnittlich 70,3 Millionen E-Mails pro Tag. Nach dem Ende der Sommerferien war das deutlich mehr, als noch im Vormonat (+55%). Darunter waren rund 43,8 Millionen Spam-Mails (62% gegenüber dem Vormonat) und 26,6 Millionen legitime, erwünschte E-Mails (+9% gegenüber dem Vormonat).

Spam-Quote:
47 % im Monatsdurchschnitt

Veränderung:
- 4 Prozentpunkte
zum Vormonat

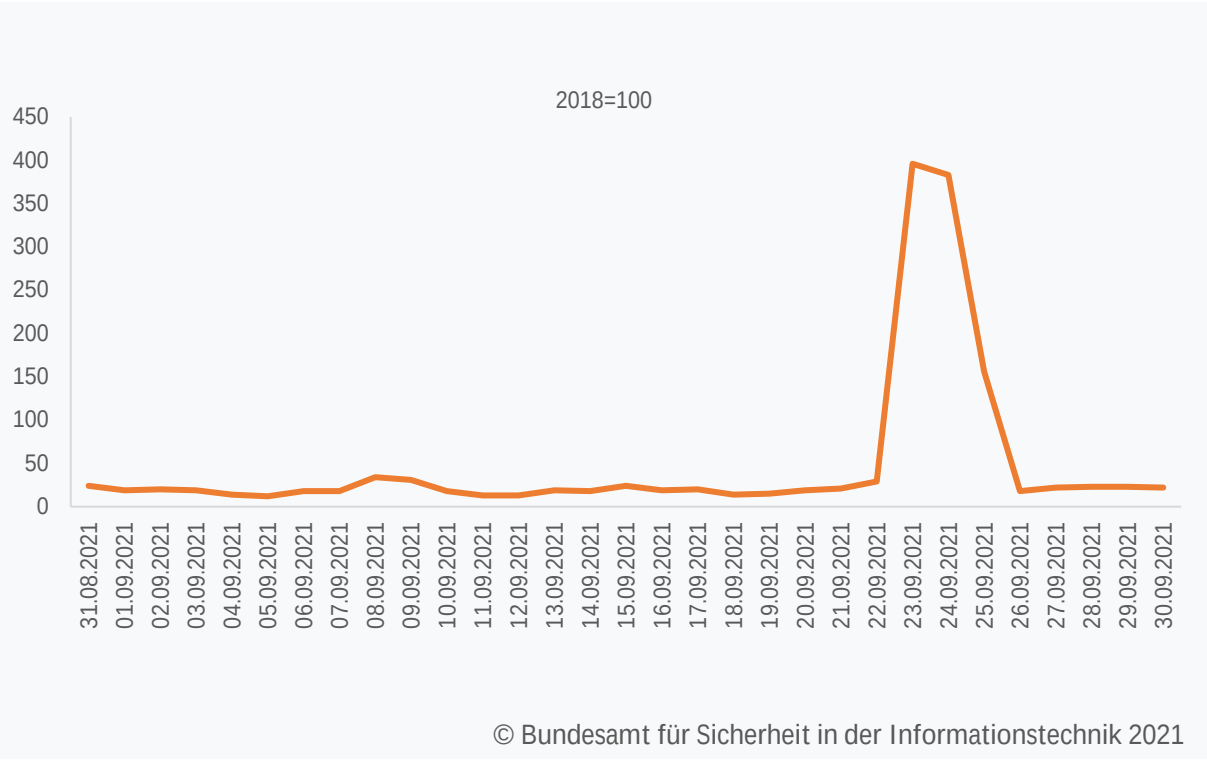
Die Spam-Quote lag im Berichtsmonat bei 47%. Das waren 4 Prozentpunkte weniger als noch im Vormonat (-4 Prozentpunkte).

Bewertung

Die Lage bei Spam-Mails war im September 2021 durchschnittlich bedrohlich. Moderne Spam-Filter konnten die meisten Spam-Mails erfolgreich abwehren, bevor sie die adressierten Opfer erreichen konnten.

Erläuterung: Für die Schätzung des E-Mail-Aufkommens in der Wirtschaft in Deutschland werden die Ergebnisse einer 2%-Stichprobe des E-Mail-Verkehrs von Unternehmen in Deutschland (Inlandskonzept) hochgerechnet. Als Spam-Mail gilt jede unerwünschte E-Mail. Dabei kann es sich sowohl um unerwünschte Werbe-E-Mails als auch um gefährlichen Malware-Spam handeln.
Quelle: E-Mail-Verkehrsstatistik

1.1.2 Spam-Mail-Index für die Wirtschaft in Deutschland im September 2021



Spam-Mail-Aufkommen im September 2021 weiter unterdurchschnittlich

Sachverhalt

Der Spam-Mail-Index, der das Aufkommen und die Entwicklung der Spam-E-Mails in der Wirtschaft in Deutschland misst, lag im September 2021 weiter auf unterdurchschnittlichem Niveau. Mit durchschnittlich 49 Punkten maß der Indikator aber 62 Prozent mehr Spam-Mails als noch im Vormonat.

Spam-Mail-Index:
49 Punkte
im Monatsdurchschnitt

Veränderung:
+ 62 % zum Vormonat

Zudem war in der 38. KW wieder eine ausgeprägte Spam-Welle aus dem Sextortion-Bereich zu beobachten. Die Cyber-Erpresser gaben vor, die Adressierten der Spam-Mails beim Besuch pornografischer Webseiten gefilmt zu haben, drohten, das angebliche Videomaterial an die Kontakte des Opfers zu versenden und versuchten, einen niedrigen vierstelligen Betrag in Bitcoin zu erpressen.

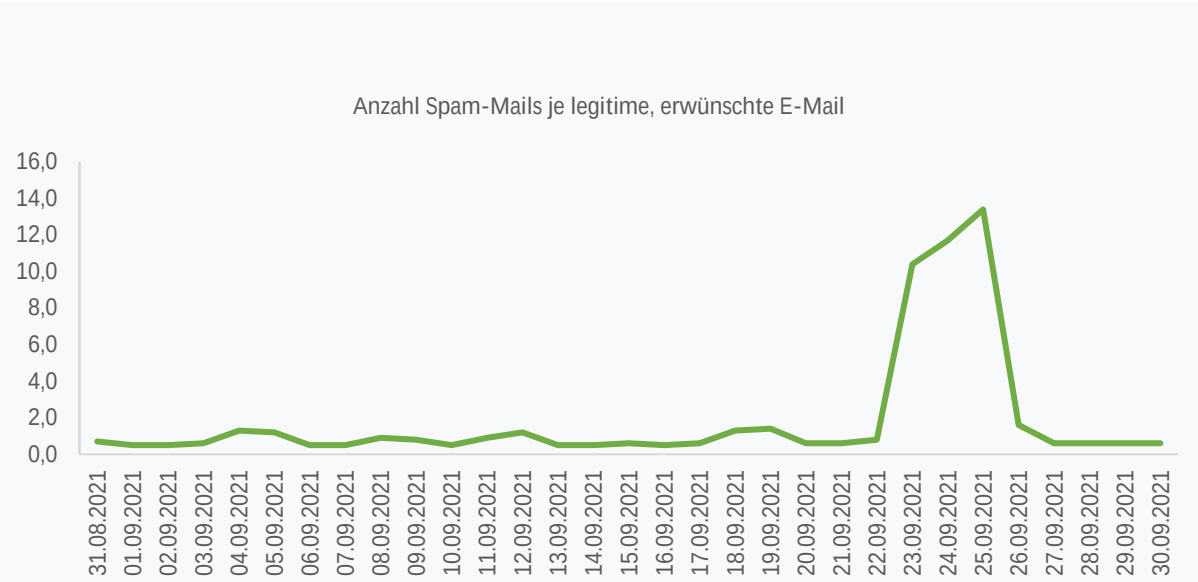
Das Ausmaß der Sextortion-Kampagne vom Ende Mai erreichte die Spam-Welle im September aber nicht.

Bewertung

Die Lage bei Spam-Mails war im September 2021 durchschnittlich. Moderne Spam-Filter konnten die meisten Spam-Mails erfolgreich abwehren, bevor sie die adressierten Opfer erreichten.

Erläuterung: Der Spam-Mail-Index für die Wirtschaft in Deutschland setzt das aktuelle Spam-Mail-Aufkommen ins Verhältnis zum Durchschnittswert des Jahres 2018 (2018=100). Die Messzahl ist unabhängig von den absoluten Werten und ermöglicht daher den direkten Vergleich der Ergebnisse über verschiedene Berichtszeiträume oder Berichtskreise hinweg. Sie eignet sich daher z.B. auch zum Benchmarking.
Quelle: E-Mail-Verkehrsstatistik

1.1.3 Spam-Ratio in der Wirtschaft in Deutschland im September 2021



Spam-Ratio unauffällig

Sachverhalt

Im September 2021 kamen auf eine legitime, erwünschte E-Mail in der Wirtschaft durchschnittlich 1,9 Spam-Mails. Eine E-Mail-Adresse, auf die im Berichtsmonat beispielsweise 100 legitime und erwünschte E-Mails eingingen, wurde also statistisch gesehen zusätzlich mit rund 190 Spam-Mails adressiert.

Abgesehen von einer Sextortion-Kampagne in der zweiten Monatshälfte zeigte die Spam-Ratio im Berichtsmonat keine Auffälligkeiten.

Monatsdurchschnitt:
1,9 Spam-Mails je legitimer, erwünschter Mail

Veränderung:
+ 28 % zum Vormonat

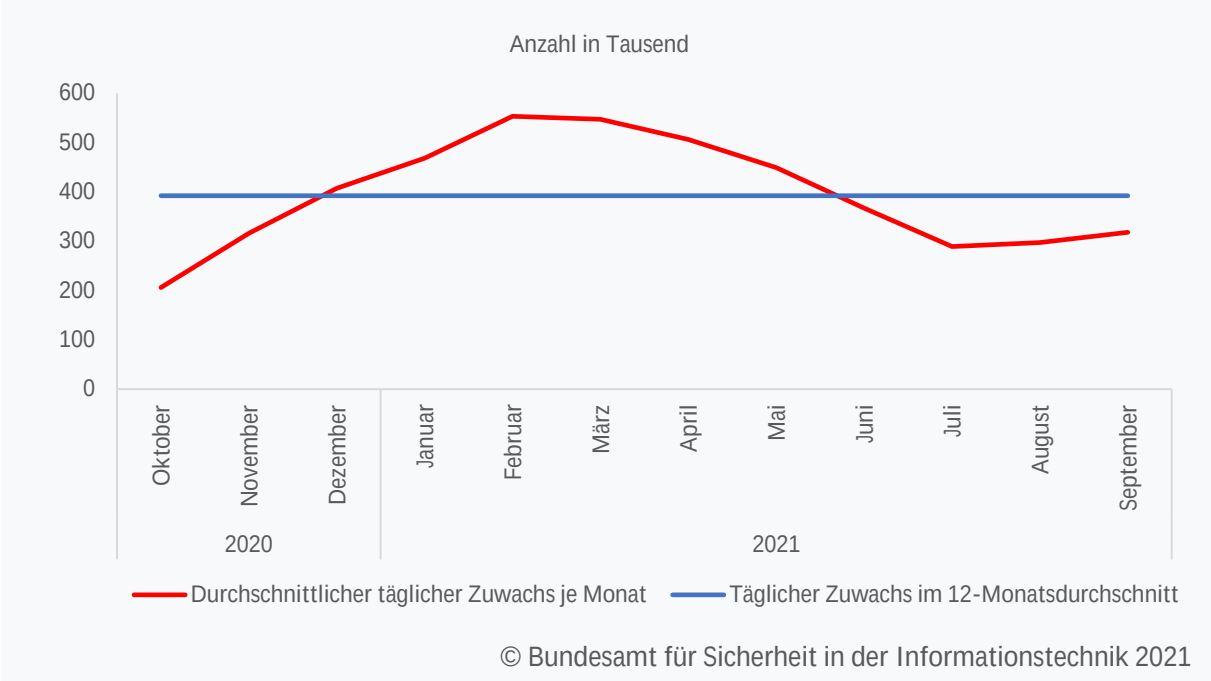
Bewertung

Die Lage bei Spam-Mails war im September 2021 durchschnittlich. Moderne Spam-Filter konnten die meisten Spam-Mails erfolgreich abwehren, bevor sie die adressierten Opfer erreichen konnten.

Erläuterung: Als Spam-Mail gilt jede unerwünschte E-Mail. Dabei kann es sich sowohl um unerwünschte Werbe-E-Mails als auch um gefährlichen Malware-Spam handeln. Die Lagebewertung erfolgt anhand der Spam-Ratio. Die Kennzahl gibt die Anzahl an Spam-E-Mails je legitime, erwünschte E-Mail im Berichtszeitraum an. Im Gegensatz zum Spam-Mail-Index reagiert die Spam-Ratio sensitiv auf das E-Mail-Verkehrsaufkommen insgesamt.
Quelle: E-Mail-Verkehrsstatistik

1.2 Malware

1.2.1 Neue Malware-Varianten insgesamt von Oktober 2020 bis September 2021



Tagesindikator für neue Malware-Varianten weiter auf unterdurchschnittlichem Niveau

Sachverhalt

Im September 2021 wurden insgesamt gut 9,5 Millionen neue Schadprogramm-Varianten bekannt. Das entsprach einem durchschnittlichen Zuwachs von gut 318.000 neuen Malware-Varianten pro Tag (+ 7 % gegenüber dem Vormonat). Nach den saisonbedingt weit unterdurchschnittlichen Wert im in den Sommermonaten weist der Indikator damit wieder leicht nach oben.

Tagesindikator:
318.000 neue Malware-Varianten pro Tag

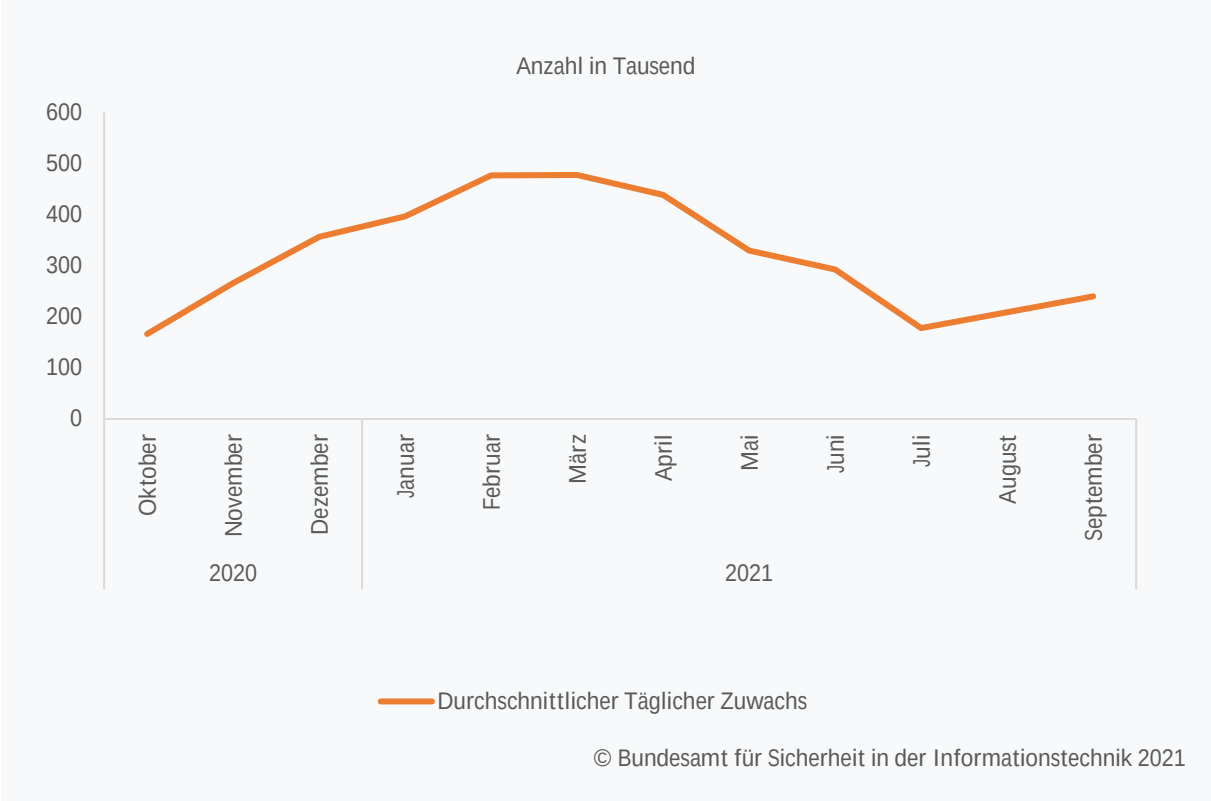
Veränderung:
+ 7 % zum Vormonat

Bewertung

Die Lage bei neuen Malware-Varianten war im September 2021 durchschnittlich bedrohlich. Wer früher bereits die meisten Malware-Angriffe erfolgreich abwehren konnte, dem gelang dies auch im Berichtszeitraum. Über die ständige Aktualisierung des bestehenden Malware-Schutzes hinaus waren keine weiteren Maßnahmen notwendig, um gegen die Bedrohung gut geschützt zu sein.

Erläuterung: Der durchschnittliche tägliche Zuwachs wird auf Basis der spitzen Monatswerte berechnet. Referenz des Indikators ist der Durchschnittswert des täglichen Zuwachses über die letzten 12 Monate. Als Malware-Variante zählt jede im Hinblick auf ihren Hashwert einzigartige Variante einer Malware.
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

1.2.2 Neue Windows-Malware-Varianten von Oktober 2020 bis September 2021



Produktion neuer Windows-Malware-Varianten wächst weiter (+15%)

Sachverhalt

Im September 2021 wurden täglich durchschnittlich 240.000 neue Windows-Malware-Varianten bekannt. Das waren rund 15 Prozent mehr neue Windows-Malware-Varianten, als noch im Vormonat. Die Menge neuer Varianten stieg damit in der Kategorie der Windows-Malware noch deutlicher als im Durchschnitt aller Malware-Kategorien.

Tagesindikator:
240.000 neue Windows-Malware-Varianten pro Tag

Veränderung:
+ 15 % zum Vormonat

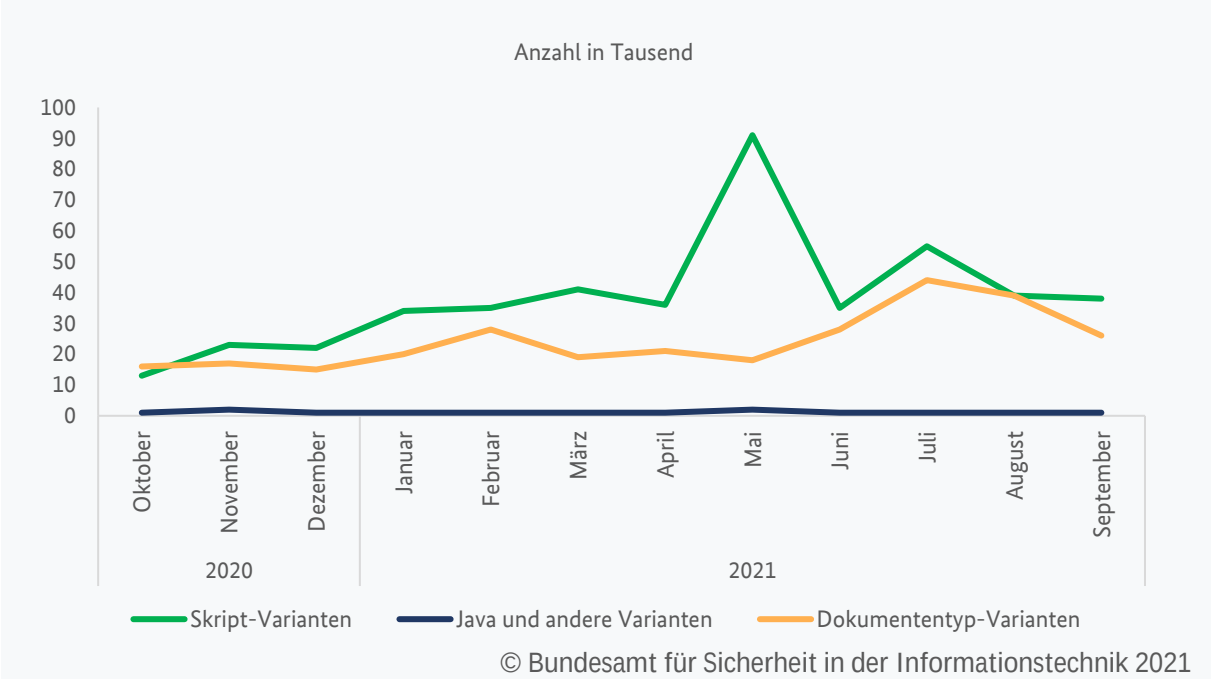
Besonders ausgeprägt war der Produktionszuwachs auch in der Kategorie der Linux-Malware (+69% zum Vormonat). Wenn auch der Anteil der Linux-Malware insgesamt weiter gering blieb, so waren im September 2021 doch erstmals seit Beginn der Zählung überhaupt statistisch signifikante Häufikgeiten zu verzeichnen (vgl. „Zahl des Monats“, Seite 4).

Bewertung

Die Lage war für Windows-Betriebssysteme im September 2021 durchschnittlich bedrohlich. Wer früher bereits die meisten Malware-Angriffe erfolgreich abwehren konnte, dem gelang dies auch im Berichtszeitraum. Über die regelmäßige Aktualisierung bestehender Schutzmaßnahmen hinaus waren in der Regel keine weiteren Maßnahmen erforderlich, um gegen die Bedrohung geschützt zu sein.

Erläuterung: Als Windows-Malware-Variante zählt jede im Hinblick auf ihren Hashwert einzigartige Variante einer Malware, die eine Schwachstelle im Windows-Betriebssystem ausnutzt. Nicht dazu zählen Varianten, die Schwachstellen in Anwendungen wie z.B. MS-Office-Anwendungen ausnutzen.
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

1.2.3 Neue Malware-Varianten für Anwendungen von Oktober 2020 bis September 2021



Produktion neuer Anwendungsmalware rückläufig

Sachverhalt

Plattformunabhängige Malware-Varianten zielen auf Schwachstellen in Anwendungen wie z.B. Browser, Office-Programme oder Reader. Insgesamt wurden im September 2021 knapp 2 Millionen neue Anwendungsmalware-Varianten bekannt. Im 12-Monatsvergleich bleibt die Produktion von Anwendungsmalware insgesamt damit weiter leicht erhöht. In der Kategorie der Dokumententypen-Varianten war aber ein deutlicher Rückgang zu verzeichen (-33%).

Tagesindikator:
38.000 neue
Skript-Varianten pro Tag

Veränderung:
- 3 % zum Vormonat

Tagesindikator:
26.000 neue
Dokumententyp-Varianten pro Tag

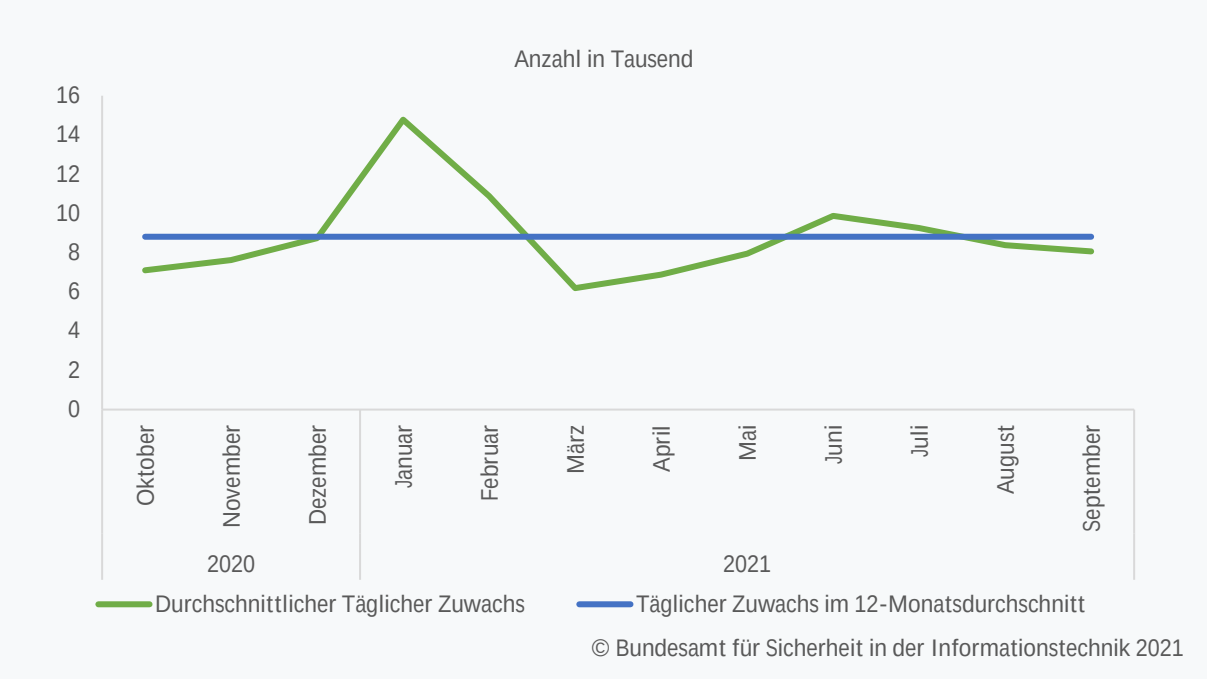
Veränderung:
- 33 % zum Vormonat

Bewertung

Die Lage für Anwendungssoftware wie Office-Programme oder Browser war im September 2021 durchschnittlich bedrohlich. Wer früher bereits die meisten Malware-Angriffe erfolgreich abwehren konnte, dem gelang dies auch im Berichtszeitraum. Über die regelmäßige Aktualisierung bestehender Schutzmaßnahmen hinaus waren in der Regel keine weiteren Maßnahmen erforderlich, um gegen die Bedrohung geschützt zu sein.

Erläuterung: Dokumententyp-Varianten gehören zu den sog. plattformunabhängigen Varianten. Im Gegensatz zu den plattformbezogenen Varianten, die Schwachstellen in Betriebssystemen ausnutzen, zielen sie auf Schwachstellen in Anwendungen wie z.B. Office-Programmen, Graphik-Programmen, Webanwendungen usw. Als Variante zählt jede im Hinblick auf ihren Hashwert einzigartige Variante.
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

1.2.4 Neue Malware-Varianten für Android-Geräte von Oktober 2020 bis September 2021



Tagesindikator bei Android-Malware nahe am 12-Monatsdurchschnitt (-4%)

Sachverhalt

Die Produktion neuer Android-Malware-Varianten ließ im Berichtsmonat weiter nach (-4% gegenüber dem Vormonat). Insgesamt waren durchschnittlich rund 8.000 neue Android-Malware-Varianten pro Tag zu verzeichnen.

Tagesindikator:
8.000 neue Android-Malware-Varianten pro Tag

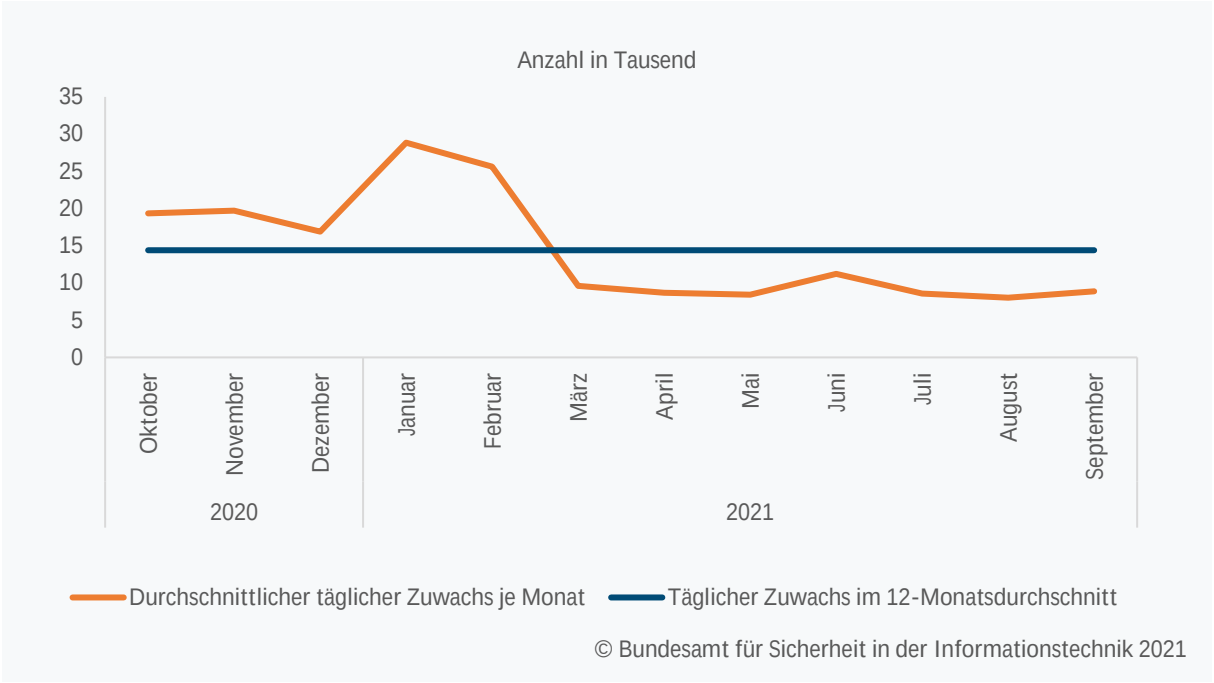
Veränderung:
- 4 % zum Vormonat

Bewertung

Die Bedrohungslage für Android-Geräte war im September 2021 durchschnittlich bedrohlich. Geräte, auf denen nur Apps aus vertrauenswürdigen Quellen installiert waren und deren Betriebssystem auf dem aktuellsten Stand war, waren gut geschützt.

Erläuterung: Zu den neuen Android-Malware-Varianten zählen alle im Hinlick auf ihren Hashwert einzigartigen Varianten von Schädlingen, die auf Schwachstellen im Android-Betriebssystem für mobile Endgeräte zielen.
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

1.2.5 Potenziell unerwünschte Anwendungen (PUA) für Windows von Oktober 2020 bis September 2021



Aufkommen an neuen PUA-Varianten für Windows weiter unterdurchschnittlich

Tagesindikator:
9.000 neue Windows-PUA-Varianten

Veränderung:
11 % zum Vormonat

Sachverhalt

Sie sammeln unbemerkt Nutzerdaten, lesen Kontaktdaten aus oder protokollieren Nutzerverhalten im Internet mit – potentiell unerwünschte Anwendungen (PUA) sind vorwiegend von mobilen Geräten bekannt, es gibt sie jedoch auch für Betriebssysteme stationärer Geräte.

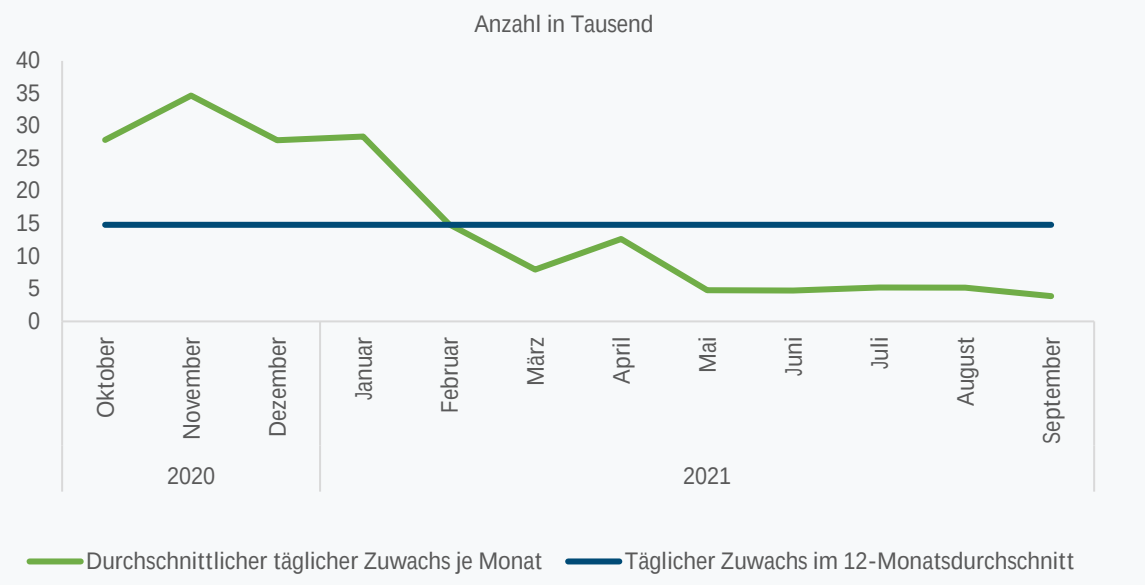
Nach einem vorübergehenden Produktionszuwachs im Juni 2021 waren nach einem deutlichen Minus im Juli 2021 auch im August und September 2021 erneut unterdurchschnittlich viele Windows-PUA-Varianten zu verzeichnen. Das waren täglich durchschnittlich rund 9.000 neue Varianten (+11% gegenüber dem Vormonat).

Bewertung

Die Bedrohung durch potentiell unerwünschte Anwendungen für Windows-Betriebssysteme war im September 2021 durchschnittlich ausgeprägt.

Erläuterung: Eine potentiell unerwünschte Anwendung (PUA) zeichnet sich dadurch aus, dass sie in der Regel vom Anwender zwar installiert wurde, jedoch ggf. nicht das erwartete Verhalten zeigt oder verdeckt Funktionen ausführt, die als „unerwünscht“ angesehen werden, z. B. Informationssammlung und ggf. Weiterleitung des Anwenderverhaltens oder Ähnliches. Als Variante zählt jede im Hinblick auf ihren Hashwert einzigartige Variante.
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

1.2.6 Potenziell unerwünschte Anwendungen (PUA) für Android von Oktober 2020 bis September 2021



Produktion neuer Android-PUA-Varianten rückläufig

Sachverhalt

Der durchschnittliche tägliche Zuwachs neuer Android-PUA-Varianten lag im September 2021 bei knapp 4.000 neuen Varianten pro Tag. Nach den ohnehin weit unterdurchschnittlichen Werten des Indikators in den Sommermonaten war damit erneut ein spürbarer Rückgang zu verzeichnen (-25% gegenüber dem Vormonat).

Tagesindikator:
4.000 neue Android-PUA-Varianten

Veränderung:
- 25 % zum Vormonat

Bewertung

Die Bedrohung durch neue Android-PUA-Varianten war im September 2021 durchschnittlich ausgeprägt. Geräte, auf denen nur Apps aus vertrauenswürdigen Quellen installiert waren und deren Betriebssystem auf dem aktuellsten Stand war, waren gut geschützt.

Erläuterung: Eine potenziell unerwünschte Anwendung (PUA) zeichnet sich dadurch aus, dass sie in der Regel vom Anwender zwar installiert wurde, jedoch ggf. nicht das erwartete Verhalten zeigt oder verdeckt Funktionen ausführt, die als „unerwünscht“ angesehen werden, z. B. Informationssammlung und ggf. Weiterleitung des Anwenderverhaltens oder Ähnliches. Als Variante zählt jede im Hinblick auf ihren Hashwert einzigartige Variante.
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

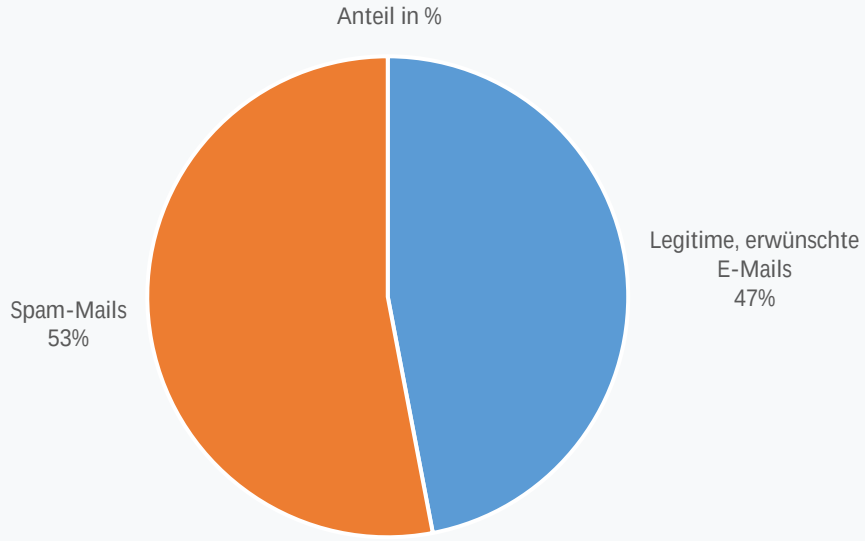
2 Schutz der Bundesverwaltung

2.1 Spam-Schutz

2.2 Malware-Schutz

2.1 Spam-Schutz in der Bundesverwaltung

2.1.1 E-Mails an die Bundesverwaltung insgesamt im September 2021



[1] Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen

Spam-Quote in der Bundesverwaltung bei 53 Prozent

Sachverhalt

Im September 2021 gingen durchschnittlich 823.000 E-Mails pro Tag in der Bundesverwaltung ein. Das waren 25 Prozent mehr als im Vormonat (+25% gegenüber dem Vormonat).

Der größere Anteil der Zunahme entfiel dabei auf die Kategorie der Spam-Mails. Hier war im September 2021 eine Zunahme von 47 Prozent gegenüber dem Vormonat zu verzeichnen.

Spam-Quote:
53 % im Monatsdurchschnitt

Veränderung:
+3 Prozentpunkte zum Vormonat

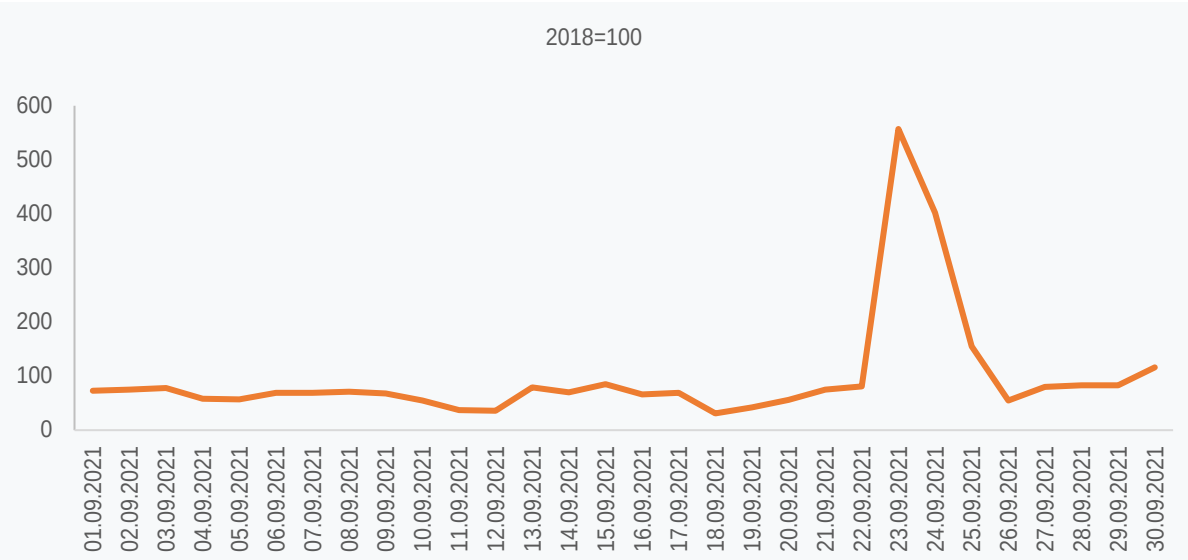
Die Spam-Quote lag im September 2021 bei durchschnittlich 53 Prozent (+3 Prozentpunkte gegenüber dem Vormonat). Das entsprach durchschnittlich gut 466.000 Spam-Mails pro Tag. Von diesen wurden 83 Prozent durch die zentralen Schutzmaßnahmen des BSI abgewehrt. Die übrigen wurden auf Wunsch der betroffenen Behörden als Spam markiert und zugestellt.

Bewertung

Die Bedrohung der Bundesverwaltung durch Spam-Mails war im September 2021 durchschnittlich ausgeprägt. Durch die zentralen Schutzmaßnahmen des BSI konnten die meisten Spam-Mails erfolgreich abgewehrt werden.

Erläuterung: Als Spam-Mail gilt jede unerwünschte E-Mail. Dabei kann es sich sowohl um unerwünschte Werbe-E-Mails als auch um Phishing-Mails oder gefährlichen Malware-Spam handeln.
Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung

2.1.2 Spam-Mail-Index für die Bundesverwaltung im September 2021



[1] Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen

Spam-Mail-Index im September 2021 bei durchschnittlichen 101 Punkten.

Sachverhalt

Der Spam-Mail-Index lag mit durchschnittlich 101 Punkten im September 2021 auf durchschnittlichem Niveau. Das entsprach einem Plus von 47 Prozent gegenüber dem Vormonat.

Der Spam-Mail-Index für die Bundesverwaltung registrierte auch die Sextortion-Spam-Wellen in der zweiten Monatshälfte (vgl. Seite 6), als der Indikator sich binnen 24 Stunden fast versiebenfachte. Das Ausmaß der Sextortion-Kampagne vom Mai diesen Jahres wurde aber nicht erreicht.

Spam-Mail-Index:
101 Punkte im Monats-durchschnitt

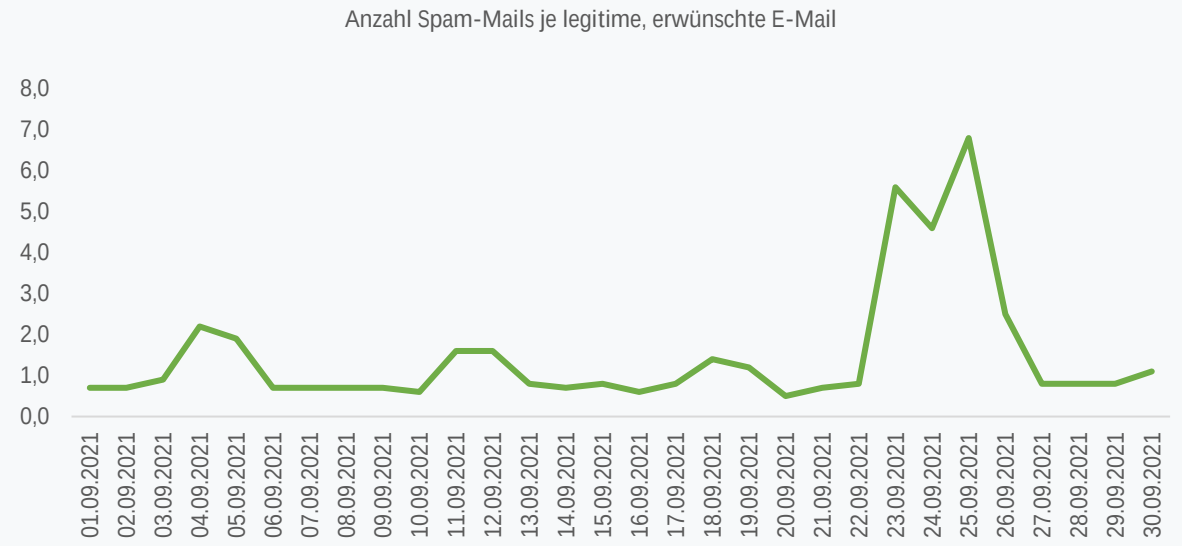
Veränderung:
+ 47 % zum Vormonat

Bewertung

Die Bedrohung der Bundesverwaltung durch Spam-Mails war im September 2021 durchschnittlich ausgeprägt. Durch die zentralen Schutzmaßnahmen des BSI konnten die meisten Spam-Mails erfolgreich abgewehrt werden.

Erläuterung: Der Spam-Mail-Index für die Bundesverwaltung setzt das aktuelle Spam-Mail-Aufkommen ins Verhältnis zum Durchschnittswert des Jahres 2018 (2018=100). Die Messzahl ist unabhängig von den absoluten Werten und ermöglicht daher den direkten Vergleich der Ergebnisse über verschiedene Berichtszeiträume oder Berichtskreise hinweg. Sie eignet sich daher z. B. auch zum Benchmarking.
Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung

2.1.3 Spam-Ratio in der Bundesverwaltung im September 2021



[1] Ohne Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen

Spam-Ratio zeigt Spam-Welle Ende September

Sachverhalt

Im September 2021 kamen in der Bundesverwaltung durchschnittlich 1,8 Spam-Mails auf eine legitime, erwünschte E-Mail. Der Indikator registrierte die Sextortion-Kampagne in der zweiten Monatshälfte, zeigte aber sonst keine Auffälligkeiten und lag überwiegend unter 1 (d.h. es gab weniger Spam-Mails als legitime, erwünschte E-Mails).

Monatsdurchschnitt:
1,8 Spam-Mails je legitimer, erwünschter Mail

Veränderung:
+ 34 % zum Vormonat

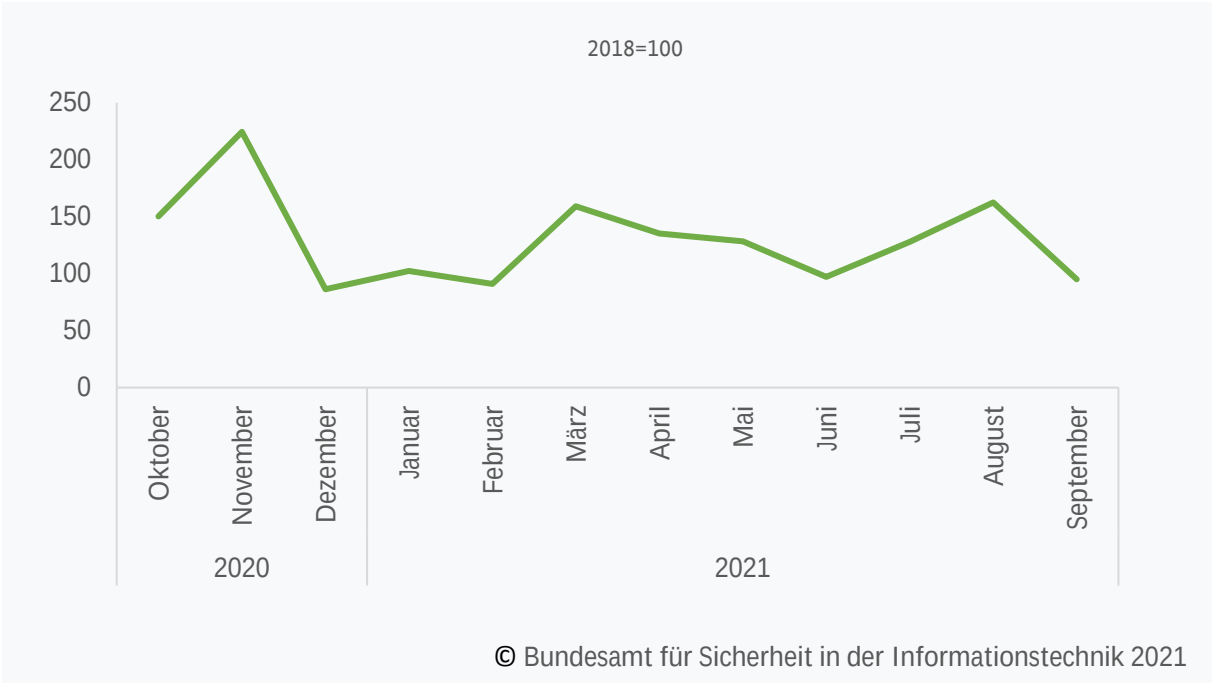
Bewertung

Die Bedrohung der Bundesverwaltung durch Spam-Mails war im September 2021 durchschnittlich ausgeprägt. Durch die zentralen Schutzmaßnahmen des BSI konnten die meisten Spam-Mails aber erfolgreich abgewehrt werden.

Erläuterung: Die Spam-Ratio gibt die Anzahl an Spam-E-Mails je legitimer, erwünschter E-Mail im Berichtszeitraum an. Im Gegensatz zum Spam-Mail-Index reagiert die Spam-Ratio sensitiv auf das E-Mail-Verkehrsaufkommen insgesamt.
Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung

2.2 Malware-Schutz in der Bundesverwaltung

2.2.1 Neue Sperrungen maliziöser Webseiten von Oktober 2020 bis September 2021



Webfilter-Maßnahmen wieder auf durchschnittlichem Niveau

Sachverhalt

Im September 2021 mussten rund 42 Prozent weniger maliziöse Webseiten gesperrt werden als noch im Vormonat (-42%). Der Index über die neuen Sperrungen maliziöser Webseiten, der bereits im August einen deutlichen Zuwachs verzeichnet hatte, normalisierte sich im Berichtsmonat bei 95 Punkten auf durchschnittlichem Niveau.

Index über die neuen Webseiten-Sperrungen bei
95 Punkten

Veränderung:
-42 % zum Vormonat

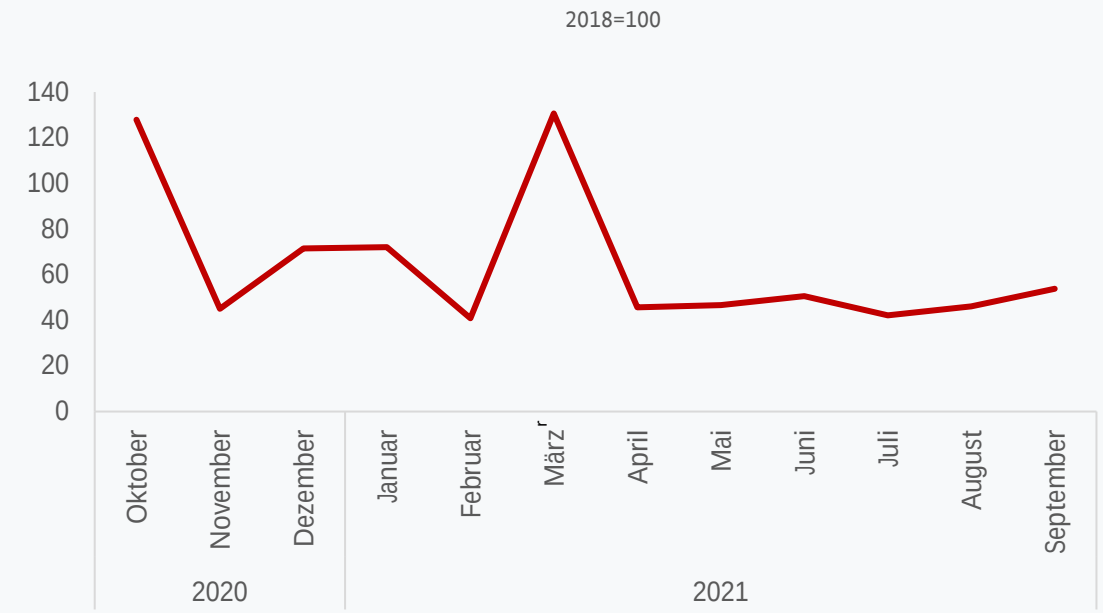
Die Sperrung einer Webseite wird nötig, wenn bekannt wird, dass Angreifer darauf Schadcode zum Download bereithalten. Dieser kann sich beispielsweise in illegalen Software-Kopien verstecken, die zum Download angeboten werden, oder auch ganz automatisch und unbemerkt beim Aufruf der Webseite installiert werden (Drive-by-Infektion). Die zentralen Schutzmaßnahmen des BSI verhindern in den Netzen der Bundesverwaltung solche Infektionen durch bekannte maliziöse Webseiten.

Bewertung

Die Bedrohung durch neue maliziöse Webseiten war im September 2021 durchschnittlich. Die an die zentralen Schutzmaßnahmen des BSI angeschlossenen Behörden waren gegen solche Angriffe gut geschützt.

Erläuterung: Der Index über die neuen Webseiten-Sperrungen gibt Auskunft über die im Berichtszeitraum nötig gewordenen neuen Webseiten-Sperrungen. Webseiten-Sperrungen sind Präventiv-Maßnahmen. Sie verhindern, dass bei der Internetnutzung aus der Bundesverwaltung heraus auf Webseiten zugegriffen werden kann, die Schadcode verbreiten. Je mehr maliziöse Webseiten bekannt werden und präventiv gesperrt werden können, desto geringer die Gefahr unbemerkter Malware-Infektionen.
Der Index setzt die Anzahl neuer Webseiten-Sperrungen ins Verhältnis zum Durchschnittswert des Jahres 2018 (2018=100). Die Messzahl ist unabhängig von den absoluten Werten und ermöglicht daher den direkten Vergleich der Ergebnisse über verschiedene Berichtszeiträume oder Berichtskreise hinweg. Sie eignet sich daher z.B. auch zum Benchmarking.
Quelle: Webfilter-Messung

2.2.2 Index über die Malware-Angriffe auf die Bundesverwaltung von Oktober 2020 bis September 2021



1 Ohne Angriffe auf Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen.
r Berichtigt.

Index über die Malware-Angriffe auf die Bundesverwaltung steigt wieder leicht

Sachverhalt

Der Index über die Malware-Angriffe per E-Mail auf die Bundesverwaltung lag im September 2021 bei 54 Punkten. Gegenüber dem Vormonat war das ein spürbarer Zuwachs um 17 Prozent. Der Indikator blieb insgesamt aber auf unterdurchschnittlichem Niveau.

Index über die Malware-Angriffe auf die Bundesverwaltung bei
54 Punkten

Veränderung:
+ 17% zum Vormonat

Bewertung

Die Lage bei Malware-Angriffen per E-Mail war im September 2021 durchschnittlich bedrohlich. Über die ständige Aktualisierung des bestehenden Malware-Schutzes hinaus waren keine weiteren Maßnahmen notwendig, um gegen die Bedrohung gut geschützt zu sein.

Erläuterung: Der Index über die Malware-Angriffe auf die Bundesverwaltung misst das Aufkommen und die Entwicklung der Cyber-Angriffe auf die Bundesverwaltung, die per E-Mail ausgeführt werden. Er gibt also das Aufkommen an E-Mails mit maliziösem Anhang an.
Quelle: Erhebung über die E-Mail-Angriffe auf die Bundesverwaltung

Glossar

E-Mail:
Eine E-Mail im Sinne der E-Mail-Verkehrsstatistik ist eine elektronisch mittels SMTP-Protokoll transportierte Nachricht eines eindeutigen Absenders an einen eindeutigen Empfänger. E-Mails lassen sich nach ihrer Art in legitime, erwünsche E-Mails einerseits sowie unerwünschte Spam-E-Mails (darunter: gefährlicher Malware-Spam) andererseits unterscheiden.

Indikator, Kennzahl:
Als Indikator wird eine messbare Variable bezeichnet, die anstelle einer nicht messbaren Variablen erhoben wird. Die nicht messbare Variable (z.B. „Bedrohungslage“, soll dabei durch eine oder mehrere messbare Variablen soweit wie möglich angenähert werden (z.B. Spam-Mail-Index, durchschnittlicher täglicher Zuwachs neuer Malware-Varianten usw.).

Legitime, erwünschte E-Mails:
Legitim und erwünscht sind autorisierte E-Mails im Rahmen der persönlichen alltäglichen elektronischen Kommunikation sowie erwünschte Massenmailings (z.B. Newsletter), die die Empfänger jederzeit mit sofortiger Wirkung kündigen können. Dazu zählen z.B. auch Werbe-Mailings, mit denen Unternehmen ihre Kunden etwa über neue Produkte oder Dienstleistungen informieren.

Malware:
Als Malware im Sinne der Malware-Statistik gilt jede Datei, die ganz oder teilweise aus Quell- oder Binärcode besteht, der auf dem befallenen System schädliche Operationen ausführen kann oder solchen Code in anderen Dateien dazu befähigen kann, schädliche Operationen durchzuführen (z.B. Nachlade-Malware).

Messzahl, Index:
Messzahlen stellen Veränderungen und Entwicklungen unabhängig von den absoluten Zahlen dar, indem die absoluten Zahlen ins Verhältnis zu einem früher gemessenen Durchschnittswert gesetzt werden. So bedeutet eine Malware-Messzahl von 120 Punkten (2018=100) beispielsweise, dass das Aufkommen an neuen Malware-Varianten 1,2 mal so hoch lag, wie im Durchschnitt des Jahres 2018. Durch die Verwendung von Messzahlen werden Trends und Entwicklungen unabhängig von den absoluten Größen direkt miteinander vergleichbar.

Neue Malware-Varianten:
Als Variante einer Malware gilt jede im Hinblick auf ihren Hashwert einzigartige Kopie einer Malware, auch wenn diese nur geringfügig verändert wurde. Im Gegensatz zu ganz neuer Malware besitzen neue Varianten von bereits bekannter Malware keine neuen Funktionalitäten. Sie stellen aber gleichwohl eine Bedrohung dar, weil neue Malware-Varianten in der Regel produziert werden, um bestehende Schutzmaßnahmen gegen bekannte Malware zu unterwandern.

PUA (Potentiell unerwünschte Anwendung):
Anwendungssoftware (oft als „Bundled“-Software vertrieben), die nicht eindeutig als Schadsoftware klassifiziert werden kann. Eine PUA zeichnet sich insbesondere dadurch aus, dass sie in der Regel vom Anwender zwar installiert wurde, jedoch ggf. nicht das erwartete Verhalten zeigt oder verdeckt Funktionen ausführt, die als „unerwünscht“ angesehen werden, z. B. Informationssammlung und ggf. Weiterleitung des Anwenderverhaltens, Einblendung von Werbung, oder Ähnliches.

Spam-E-Mails:
Zu den Spam-E-Mails zählen alle unerwünschten E-Mails. Dabei kann es sich um unerwünschte Werbe-E-Mails, aber auch um gefährlichen Malware-Spam handeln. Die meisten Spam-E-Mails werden durch Spam-Filter von IT- und E-Mail-Dienstleistern zentral abgewehrt und erreichen die Adressierten nicht.

Spam-Ratio:
Die Spam-Ratio ist eine Messzahl, die die Zahl der Spam-E-Mails ins Verhältnis zur Zahl der legitimen, erwünschten E-Mails setzt. Der Wert sagt nichts über das absolute Spam-Mail-Aufkommen aus. So bedeutet beispielsweise ein Spam-Ratio-Wert von 4, dass im Berichtszeitraum auf jede legitime, erwünschte E-Mail vier Spam-E-Mails kamen. Das tatsächliche Aufkommen kann bei 4:1, bei 8:2 oder auch bei 1 Mio:250.000 gelegen haben. Je größer die Spam-Ratio, desto größer das Spam-Aufkommen im Vergleich zu legitimen, erwünschten E-Mails. Entwickelt sich die Spam-Ratio gegen 1, so wird der Unterschied gering. Werte unter 1 zeigen an, dass mehr legitime, erwünschte E-Mails als Spam-E-Mails zu verzeichnen waren. An Wochenenden und Feiertagen steigt die Spam-Ratio üblicherweise sprunghaft, weil der legitime, erwünschte E-Mail-Verkehr an bundesweit arbeitsfreien Tagen in der Regel deutlich nachlässt. Auffällig sind dagegen hohe Spam-Ratios an Werktagen oder über mehrere Tage hinweg.

Täglicher Zuwachs:
Der durchschnittliche tägliche Zuwachs ist eine Kennzahl für die Menge neuer Malware-Varianten, die Angreifer in einem Berichtszeitraum produziert haben. Je höher der durchschnittliche tägliche Zuwachs, desto mehr Varianten wurden produziert und desto größer die Bedrohung durch diese neuen Varianten.

Quellenverzeichnis

Indikator	Quelle
E-Mail-Aufkommen in Deutschland	E-Mail-Verkehrsstatistik
Spam-Mail-Index für Deutschland	E-Mail-Verkehrsstatistik
Spam-Ratio für Deutschland	E-Mail-Verkehrsstatistik
Neue Malware-Varianten	Malware-Statistik des BSI auf der Basis von Rohdaten des Instituts AV-Test GmbH
Neue PUA-Varianten	Malware-Statistik des BSI auf der Basis von Rohdaten des Instituts AV-Test GmbH
E-Mail-Aufkommen in der Bundesverwaltung	Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung
Spam-Mail-Index für die Bundesverwaltung	Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung
Spam-Ratio der Bundesverwaltung	Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung
Neue Sperrungen maliziöser Webseiten	Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung
Malware-Angriffe auf die Bundesverwaltung	Erhebung über die E-Mail-Angriffe auf die Bundesverwaltung

Weitere Quelle: https://www.trendmicro.com

Impressum:

Bundesamt für Sicherheit in der Informationstechnik
Referat OC 23 – Nationales IT-Lagezentrum, Analysen und Prognosen
Postfach 20 03 63
53175 Bonn

Tel.: +49 228 99 9582-6227
E-Mail: statistik@bsi.bund.de

Internet: https://www.bsi.bund.de