

## VERDÄCHTIGE POSTSENDUNGEN:

### MODERNE POSTEINGANGS- KONTROLLE DURCH (SICHERHEITS-)TECHNISCH GESTÜTZTE LÖSUNGEN



Der Austausch von Informationen findet heutzutage häufig über digitale Plattformen wie E-Mail oder Messenger-Dienste statt. Dennoch gibt es wichtige Dokumente, persönliche Briefe oder amtliche Unterlagen, die per Post zugestellt werden (müssen). Der Versand von Päckchen und Paketen hat in den vergangenen Jahren – nicht zuletzt durch diverse Onlinedienste – sogar zugenommen. Daher besteht auch weiterhin die Gefahr, dass mittels Brief, Päckchen oder Paket gefährliche (explosive) Inhalte versendet werden.

Der Auszug der Briefbomben(-anschläge) der vergangenen Jahre verdeutlicht einmal mehr, wie latent die Gefahr ist, und zwar für jeden von uns, der Brief- und Postsendungen öffnet. Die Anzahl nicht bekanntgewordener Briefbombenanschläge ist laut inoffiziellen Informationen aus den Sicherheitsbehörden deutlich höher. Gleiches gilt für die Anzahl an Postsendungen mit gefährlichen Gegenständen. Dies können z. B. Messer oder auch Rasierklingen sein, die den Adressaten beim Öffnen der Sendung verletzen sollen. Aber auch der Versand von Betäubungsmitteln auf dem Postweg ist keine Seltenheit und sollte entsprechend detektiert werden können.

#### GEFAHREN UND RISIKEN DURCH GEFÄHRLICHE POSTSENDUNGEN

Insbesondere Mitarbeiter/-innen in den Poststellen von Unternehmen, Organisationen oder öffentlichen Einrichtungen wie beispielsweise Ministerien, Behörden, Botschaften, Justizvollzugsanstalten, Gesundheitsämtern oder bei Betreibern kritischer Infrastrukturen sind latent bedroht. Aber auch alle anderen Personen, die Briefe, Päckchen oder Pakete öffnen, wie beispielsweise Assistenzen, Sekretariate, Kollegen der Empfänger und natürlich die Empfänger selbst, können mitunter gefährdet sein.



Briefbombe in Paris an den Internationalen Währungsfonds (IWF) im Jahr 2017

Serie von 16 Briefbomben an prominente Demokraten und Kritiker von Donald Trump in den USA im Jahr 2018

Mehrere Briefbomben an diverse Empfänger in London im Jahr 2019

Briefbombenfund im Kanzleramt im Jahr 2019

Serie von 11 Briefbomben in den Niederlanden seit Anfang des Jahres 2020

**BEKANTGEWORDENE BRIEFBOMBEN(-ANSCHLÄGE)  
JÜNGSTER VERGANGENHEIT**

## ” HUNDERTE BRIEFE, PÄCKCHEN UND PAKETE KOMMEN IN UNTERNEHMEN, BEHÖRDEN UND ORGANISATIONEN TÄGLICH AN – DARUNTER IN SELTENEN FÄLLEN AUCH SOLCHE MIT GEFÄHRLICHEM INHALT.

Den typischen Empfänger von Briefbomben gibt es genauso wenig wie den typischen Versender von Briefbomben. Aber die Vergangenheit zeigt, dass insbesondere Politiker/-innen und Prominente bzw. in der Öffentlichkeit stehende Personen, aber auch Entscheidungsträger, die schnell zu „Gegnern“ werden können, betroffen sind. Die Tatmotive reichen von extremistischen oder politischen Hintergründen bis hin zu kriminell motivierten oder emotionalen und persönlichen Taten.

### ERKENNUNGSMERKMALE VERDÄCHTIGER POSTSENDUNGEN

Viele Postsendungen werden heutzutage noch per Hand kontrolliert, also durch optische und haptische Prüfung. Um verdächtige Sendungen zu erkennen, gibt es einige Merkmale, die auf eine verdächtige Postsendung hinweisen können wie z. B.:

- ungewöhnliche Dicke oder Form
- hohes Gewicht bezogen auf die Größe der Postsendung
- optisch passt die Postsendung nicht mit dem vermuteten Inhalt überein
- unübliches/übertriebenes Verpackungsmaterial
- Unebenheiten bzw. fühlbare, harte Gegenstände im Inneren des Umschlags
- ölige Flecken oder Verfärbungen
- strenger/außergewöhnlicher Geruch
- Postsendung ist über das notwendige Maß hinaus frankiert
- ungewöhnliche Zustellungsart (Postsendung wurde nicht durch einen kommerziellen Zusteller ausgeliefert)
- fehlerhafte Empfängeradresse
- Angabe eines Titels, aber keine Namensangabe des Empfängers
- Rechtschreibfehler
- Hinweise wie „Vertraulich“, „Persönlich“, „Privat“, „Nur vom Empfänger zu öffnen“
- fehlender, seltsamer, unbekannter bzw. nicht existenter Absender
- anderer Aufgabeort als im Absender vermerkt

**Ein entsprechendes Merkblatt haben wir in unserem Downloadbereich für Sie zur Verfügung gestellt.**



Diese Erkennungsmerkmale sind heutzutage kein Geheimnis und somit auch den Versendern von gefährlichen Postsendungen bekannt. Daher ist die manuelle Kontrolle von Postsendungen nicht immer die beste Variante, da die potenziellen Täter die o. g. Merkmale möglichst auszuschließen versuchen. Händische Prüfungen haben oftmals auch das Problem, dass die Postsendungen zusätzlichen mechanischen Belastungen ausgesetzt werden, die zu einer Explosion oder zur Freisetzung von Gefahrstoffen führen können. Letztlich erhöht die händische Prüfung die Gefahr für die prüfenden Personen.

### MEHR SICHERHEIT DURCH TECHNISCH GESTÜTZTE POSTEINGANGSKONTROLLE

Um die Sicherheit der Posteingangskontrolle zu erhöhen bzw. potenzielle Gefahren zu reduzieren, gibt es sogenannte „Postscanner“, die Briefe und kleine Päckchen – ohne dass diese geöffnet werden müssen – auf Gefahren hin überprüfen. Postscanner visualisieren die Objekte in den Sendungen, wodurch sich Rückschlüsse auf gefährliche Substanzen ziehen lassen.

Neue Technologien technischer Kontrollmethoden können gänzlich auf Röntgenstrahlung verzichten, da sie beispielsweise mit Terahertz-Frequenzen (THz) arbeiten – ähnlich wie Sicherheitsscanner an Flughäfen – und somit aufgrund der geringen Energie für den Menschen ungefährlich sind. Da die Geräte der neuesten Generation nur noch über eine 230 Volt-Steckdose betrieben werden und die Größe eines Druckers aufweisen, sind sie leicht zu transportieren und somit auch für Räumlichkeiten mit wenig Platz gut geeignet. >>>



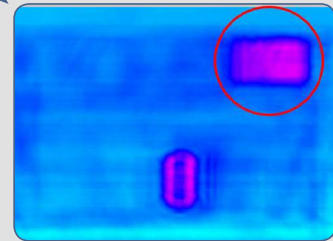
## VERGLEICH RÖNTGENANSICHT UND THZ-SCANNER



Röntgenansicht



Postsendung



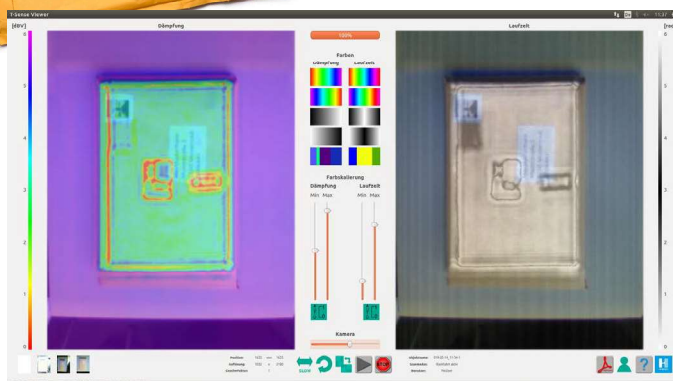
THz-Scanner

Röntengeräte nutzen für den Menschen schädliche Röntgenstrahlung (trotz deren Abschirmung) und benötigen entsprechende Abnahmen, verstärkte Schulungen der Mitarbeiter, Überprüfungen durch Prüfvereine, besondere Anforderungen an die Aufstellflächen und dergleichen. Das bedeutet: trotz der bewährten Technik ist der zusätzliche Aufwand nicht zu unterschätzen.

**WAS SIND TERAHERTZWELLEN?**  
THz-Wellen stehen im Wesentlichen für den Frequenzbereich des elektromagnetischen Spektrums zwischen 0,1 THz und 10 THz. Viele elektrisch nichtleitende Materialien können durchdrungen und somit optisch dargestellt werden. Somit lassen sich Gegenstände in Postsendungen farblich kodiert und in unterschiedlichen Ansichten auf dem Bildschirm darstellen und verborgene, kleine, interne Strukturen und unterschiedliche Materialien in der Sendung werden sichtbar. Beim Durchleuchten des Materials wird neben der Absorption auch die Laufzeit des ausgesendeten Signals durch das Material hindurch gemessen. Dadurch können geringste Unterschiede detektiert werden.

Ein weiterer technischer Vorteil von Terahertz-Scannern gegenüber herkömmlichen vergleichbaren Röntgengeräten ist, dass dünnere Pulverlagen mit THz-Wellen aufgrund der hohen Sensitivität besser erkannt werden können. Des Weiteren bieten derartige Systeme die Überlagerung von Originalbild und gescanntem Bild an, um Bereiche mit gefährlichen Gegenständen besser zuordnen zu können.

Diese Information kann beispielsweise an den Empfänger weitergegeben werden mit der Frage, ob eine solche Sendung erwartet wird oder diese direkt an die Ermittlungsbehörden übergeben werden soll.



Überlagerung original und gescanntes Bild

Bildquelle: HÜBNER GmbH & Co. KG

## VORTEILE FÜR ANWENDER

Der Einsatz von gesundheitlich unschädlichen THz-Scannern bei der Posteingangskontrolle hat viele Vorteile für den Anwender, wie z. B.:

- keine Röntgenstrahlung (dadurch keine Anforderungen aus dem Strahlenschutz)
- hoher Durchsatz (bis zu 1.000 Briefe pro Stunde)
- kurze Einweisungsdauer
- mehr Sicherheit für das Personal
- hohe Mobilität der Geräte
- Inhaltsprüfung, ohne das Postgeheimnis zu berühren
- hohe Sensitivität bei dünnere Pulverlagen
- intuitive Bedienung
- Überlagerung von Originalbild und gescanntem Bild

Trotz der technischen Möglichkeiten ist es essenziell, Mitarbeiter der Posteingangskontrolle auf das Gefährdungspotenzial hinzuweisen und entsprechend im Erkennen



## VERHALTENSGELN BEIM AUFFINDEN VERDÄCHTIGER POSTSENDUNGEN

- Ruhe bewahren!
- Kein Risiko eingehen!
- Die verdächtige Postsendung
  - ... nicht berühren!
  - ... nicht abtasten!
  - ... nicht bewegen!
  - ... nicht schütteln!
  - ... nicht biegen oder knicken!
- Keine Öffnungsversuche jedweder Art unternehmen.
- Keiner extremen Hitze (z. B. Heizung oder direkte Sonneneinstrahlung) oder Kälte aussetzen.
- Keine Mobiltelefone oder Funkgeräte in unmittelbarer Nähe verwenden.
- Gegenstand/Sendung nicht ins Wasser legen oder anfeuchten.
- Alle Personen zum Verlassen des Gefahrenbereichs (z. B. Poststelle, Büro) auffordern und den Bereich absperren (lassen) und dann auch selbst den Gefahrenbereich verlassen.
- Unverzüglich die internen Sicherheitsprozesse einleiten, wie z. B. die interne Notfallnummer und/oder die Polizei anrufen.
- Nach dem Eintreffen der Sicherheitskräfte bzw. Polizei/Feuerwehr, diese über die Erkenntnisse und bisherigen Maßnahmen umfassend informieren.



©yuriyolub - stock.adobe.com

und Umgang mit verdächtigen (explosiven) Post- und Paketsendungen zu sensibilisieren. Denn nicht selten kann die Nichtentdeckung gefährlicher (explosiver) Gegenstände zu einer massiven Gefährdung für Leib und Leben führen – daher ist die erste Reaktion oftmals entscheidend für den weiteren Verlauf.

Dem Erkennen von verdächtigen Postsendungen kommt auch zukünftig eine wichtige Aufgabe zu, die sich mit technischen Mitteln unterstützen lässt, um Unternehmen, Behörden und Organisationen bestmöglich zu schützen

Dieser Artikel ist mit freundlicher Unterstützung von Thorsten Sprenger, Head of Terahertz-Technology & Photonics der HÜBNER GmbH & Co. KG, entstanden.

### KOSTENFREIES E-LEARNING-TRAINING > UMGANG MIT BOMBENDROHUNGEN, VERDÄCHTIGEN POSTSENDUNGEN UND GEGENSTÄNDEN <

Senden Sie einfach eine E-Mail mit dem Betreff „E-Learning - verdächtige Postsendungen“ an [redaktion@sicherheit-das-fachmagazin.de](mailto:redaktion@sicherheit-das-fachmagazin.de) und Sie erhalten einen kostenfreien E-Learning-Zugang\*.

\*Maximal 1 personenbezogener Zugang pro Unternehmen.  
Gültigkeit 2 Wochen ab Erhalt der Zugangsdaten.

*„Wir sind Penetrations-  
tester. Wir finden  
Sicherheitslücken, bevor  
andere sie ausnutzen.“*



SySS GmbH  
Schaffhausenstraße 77  
72072 Tübingen  
+49 (0)7071 - 40 78 56-0  
[info@syss.de](mailto:info@syss.de)  
[www.syss.de](http://www.syss.de)