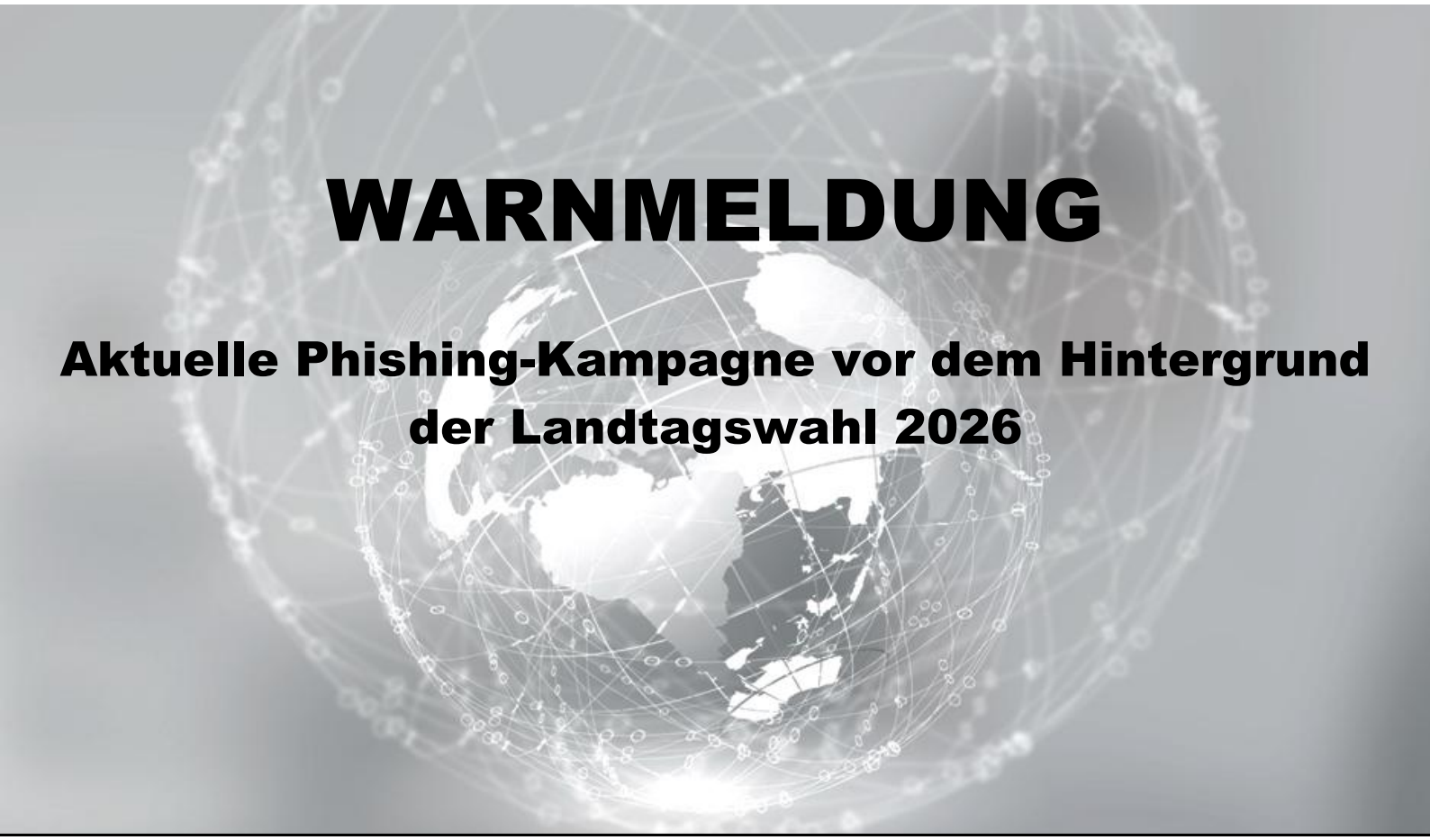
Verfassungsschutz
Baden-Württemberg

TLP:CLEAR

Beobachten.
Informieren.
Schützen.

WARNMELDUNG

Aktuelle Phishing-Kampagne vor dem Hintergrund der Landtagswahl 2026



Datum	**Ausgabe**	**Einstufung**
3. Dezember 2025	Dezember 2025	TLP:CLEAR

Landesamt für Verfassungsschutz
Baden-Württemberg
Cyberabwehr
Taubenheimstraße 85A • 70372 Stuttgart
Telefon 0711 9544 4985
E-Mail Cyberabwehr@lfvbw.bwl.de

Verfassungsschutz
Baden-Württemberg

Beobachten.
Informieren.
Schützen.

Aktuelle Phishing-Kampagne vor dem Hintergrund der Landtagswahl 2026

1. Kurzfassung

Politikerinnen und Politiker stehen besonders im Fokus der Öffentlichkeit und damit auch im Visier von Cyberkriminellen. Aktuelle Sicherheitsanalysen zeigen, dass Angriffe auf politische Akteure subtiler werden.
Neben klassischen Phishing-E-Mails nutzen Angreifer vermehrt eine Methode, die auf menschlicher Unachtsamkeit und kleinen Tippfehlern basiert, dem sogenannten Typosquatting.
Vor dem Hintergrund der Wahl zum 18. Landtag von Baden-Württemberg am 8. März 2026, informiert die Cyberabwehr des Landesamts für Verfassungsschutz nachfolgend zu den damit einhergehenden Gefahren und wie Sie sich davor schützen können:

2. Die neue Betrugsmasche

Angreifer registrieren Internetadressen, die auf den ersten Blick wie vertrauenswürdige Microsoft-Login-Seiten aussehen. Sie spekulieren darauf, dass Sie sich vertippen oder einen Link nicht genau prüfen. Dabei nutzen sie eine optische Täuschung im Schriftbild, dem sogenannten Kerning.
Die Buchstabenkombination „r“ und „n“ verschmilzt in vielen Schriftarten zu einem „m“. So wird beispielsweise aus dem Original microsoft.com die Fälschung rnicrosoft.com. Bei genauer Betrachtung erkennt man die Fälschung des ersten Buchstabens. Es handelt sich dabei nicht um ein „m“, sondern um ein „r“ gefolgt von einem „n“.

Weitere häufig vorkommende Täuschungen:

- Tausch des Buchstabens „i“ mit dem Buchstaben „l“ (kleines L).
- Tausch des Buchstabens „O“ mit der Zahl „0“.
- Tausch der Schreibweise des Buchstabens „a“ mit der Schreibweise „a“

Beim schnellen Lesen überfliegt das Gehirn das Wort bzw. korrigiert den Fehler automatisch. Insbesondere auf kleinen Smartphone-Displays ist dieser Unterschied fast nicht zu erkennen. Zudem blenden mobile Browser die Adresszeile oft teilweise aus. Landen Sie auf der gefälschten Seite, sieht diese oft nahezu identisch aus wie das Original. Geben Sie dort Ihre Zugangsdaten ein, werden diese direkt an die Angreifer übermittelt.

3. Warum ist das gefährlich?

Die Konsequenzen eines erfolgreichen Angriffs können gravierende Auswirkungen haben. Die Angreifer erhalten Zugriff auf Ihre (internen) E-Mails, Kontaktinformationen und vertrauliche Daten. Sie sind dadurch in der Lage, in Ihrem Namen Nachrichten zu versenden und beispielsweise Desinformation zu verbreiten. Darüber hinaus droht ein empfindlicher Reputationsschaden, wenn vertrauliche Informationen durch ein solches Leck an die Öffentlichkeit geraten. In der Vergangenheit kam es bereits im Rahmen von Wahlen zu solchen Hack-and-Leak- bzw. Hack-and-Publish-Angriffen.

4. Handlungsempfehlung

- Fahren Sie mit der Maus über Links in E-Mails *ohne* darauf zu klicken. Prüfen Sie im erscheinenden kleinen Fenster die Schreibweise der Zieladresse buchstabengenau.
- Wenn Sie aufgefordert werden, Ihr Passwort zu ändern oder eine Rechnung zu prüfen, klicken Sie ***nicht*** auf den mitgelieferten Link. Öffnen Sie Ihren Browser und tippen Sie die Adresse manuell ein.
- Klicken Sie in der E-Mail auf den Namen des Absenders, um die tatsächliche E-Mail-Adresse dahinter zu sehen.
- Schauen Sie sich die Adresse im Browser genau an, bevor Sie Passwörter eingeben. Achten Sie auf Buchstabendreher, doppelte Buchstaben oder falsche Endungen (z.B. .com statt .de).
- Tippen Sie wichtige Adressen nicht jedes Mal neu ein. Nutzen Sie Lesezeichen (Bookmarks) im Browser.
- Seien Sie skeptisch, wenn Sie per Mail aufgefordert werden, sich dringend irgendwo einzuloggen, selbst wenn der Absender bekannt scheint. Führen Sie immer eine Plausibilitätsprüfung durch.
- Nutzen Sie überall, wo es möglich ist, eine mehrstufige Anmeldung. Selbst wenn ein Angreifer Ihr Passwort durch Typosquatting erbeutet, kommt er ohne den zweiten Faktor (z.B. Code auf dem Handy) nicht in Ihren Account.
- Auf Mobilgeräten können Sie sich durch langes Drücken und Gedrückthalten des Links die tatsächliche Ziel-URL anzeigen lassen.
- Die Analyse von E-Mail-Headern kann Aufschluss darüber geben, ob es sich bei der E-Mail um eine Phishing-Mail handelt.

5. Fazit

Digitale Sicherheit ist Voraussetzung für eine souveräne Amtsführung. Im hektischen Wahlkampf- oder Parlamentsalltag kann ein flüchtiger Klick weitreichende Folgen haben. Die aktuelle Welle an „rnicrosoft“-Domains zeigt, dass die Angreifer gezielt auf unsere menschliche Wahrnehmung setzen. Ein kurzer, kritischer Blick auf die Adresszeile kann genügen, um einen schwerwiegenden Datenabfluss zu verhindern.

Die Cyberabwehr hat im Vorfeld der anstehenden Landtagswahl bereits am 24. November einen Sicherheitshinweis zur aktuellen Phishing-Kampagne veröffentlicht. Das Schreiben finden Sie auf unserer Homepage unter diesem **Link**.

6. Kontakt

Sollten Sie eine entsprechende Betroffenheit feststellen oder Rückfragen haben, steht Ihnen die Cyberabwehr unter den folgenden Erreichbarkeiten zur Verfügung. Bei Kontaktaufnahme kann Ihnen seitens des Verfassungsschutzes Vertraulichkeit zugesichert werden.

Telefon: 0711 9544 4985

E-Mail: Cyberabwehr@lfvbw.bwl.de

Zum Senden verschlüsselter E-Mails finden Sie **hier** unseren öffentlichen PGP-Schlüssel.

7. Weitergabevorbehalt

TLP:CLEAR Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.