



Newsletter

Liebe Kunden und Geschäftspartner,

Weihnachten und das Jahresende sind die perfekte Zeit, um Ihnen allen für Ihre langjährige Treue und Unterstützung ganz herzlich zu danken.

Das ganze Team der ETL consit wünscht Ihnen und Ihren Lieben fröhliche Festtage und ein erfolgreiches und gesundes Jahr 2026.

In unserem letzten Newsletter im Jahr 2025 informieren wir Sie insbesondere zu aktuell anstehenden Herausforderungen im kommenden Jahr:

- Cybersecurity aktuell: Es passiert nicht nur den anderen – wie du dich jetzt schützt
- WpI-MaRisk kommt!
- Fit für Prävention von Geldwäsche und Terrorismusfinanzierung 2027
- Risk in Focus 2026 des DIIR
- DORA-Informationsregister
- EU plant „Digital Omnibus“-Paket – Weniger Bürokratie, klarere Datenschutzregeln!

Auf bald im neuen Jahr!

Bernd Schmid

Oliver Gose

Cybersecurity aktuell: Es passiert nicht nur den anderen – wie du dich jetzt schützt

Stell dir vor, ...



... du willst morgens schnell deine E-Mails checken, eine Überweisung erledigen oder die Hotelbuchung für den Weihnachtsurlaub abschließen. Plötzlich reagiert nichts mehr – stattdessen erscheint eine Lösegeldforderung. Deine Fotos, Dokumente und Zugangsdaten? Verschlüsselt. Und das alles, weil ein einziges Passwort schwach war oder ein Update nicht installiert wurde.

Das klingt weit hergeholt? Leider nicht: Im letzten Jahr gab es **461 Datenleaks – mit Millionen sensibler**

Datensätze von deutschen Institutionen und Verbraucherinnen und Verbrauchern. Betroffen waren u. a. Geburtsdaten (92 %), Adressen (72 %) und Passwörter.

Warum das Thema uns alle betrifft

Die Lage der IT-Sicherheit bleibt angespannt. Cybercrime ist längst kein Hobby mehr, sondern ein globales Geschäft. Die weltweiten Kosten sollen 2025 die Marke von **10 Billionen US-Dollar (10.000.000.000.000 \$) erreichen**. In Deutschland betrug der Schaden allein 2024 rund **178,6 Milliarden Euro** – 20 % mehr als im Vorjahr. Tendenz steigend.



¹World Economic Forum (2025). Global Cybersecurity Outlook.

²Bitkom (2024). Angriffe auf die deutsche Wirtschaft nehmen zu.

Gerade vor Weihnachten steigt die Gefahr: Betrüger nutzen die Zeit für gefälschte Shops, Phishing-Mails und Fake-Buchungsportale. Ein Klick kann reichen, um Geld und Daten zu verlieren.

Die neuen Spielregeln der Angreifer

- **KI-gestützte Angriffe:** Deepfakes, automatisierte Phishing-Kampagnen und verschleierte Angriffsstrategien machen Erkennung extrem schwierig.
- **Multi-Channel-Angriffe:** Nicht nur E-Mail – auch Messenger, Social Media und sogar Telefonanrufe werden genutzt.

- **Angriffe auf persönliche Identitäten:** Private Geräte und Konten sind das perfekte Einfallstor.

Privates ist genauso gefährdet wie Berufliches

Oft sogar mehr – weil wir zu Hause keine IT-Abteilung haben, die uns möglicherweise retten könnte.

Aber Achtung: Das ist ein Irrglaube. Auch die beste IT-Abteilung kann nicht alles verhindern und selbst Unternehmen sind nie zu 100 % geschützt. **Sicherheit ist immer eine gemeinsame Verantwortung.**

So schützt du dich – gerade jetzt

Patchen, patchen, patchen: Updates sofort installieren – auf PC, Smartphone und IoT-Geräten.

Was ist IoT? Internet of Things (IoT) sind mit dem Internet verbundene Geräte, die wir gerne aus den Augen verlieren – wie z. B. Amazon Alexa, smarte Lampen oder Temperatursteuerungen. Auch diese Geräte müssen regelmäßig aktualisiert werden, um Sicherheitslücken zu schließen.

Starke Passwörter & 2FA: Nutze Passwortmanager und aktiviere Zwei-Faktor-Authentifizierung. Im Unternehmen verwenden wir **Microsoft Authenticator**, der einfach zu bedienen ist und auch privat genutzt werden kann. Alternativen sind z. B. **Google Authenticator** oder moderne **Passkeys**, die eine noch sicherere Anmeldung ermöglichen.

Als Passwortmanager ist [KeePass](#) beliebt und sicher. In der Apple-Welt eignet sich ["Passwörter"](#) (ehemals iCloud-Schlüsselbund) für MacOS und iOS sehr gut.

Augen auf bei E-Mails & Links: Keine Anhänge oder Links öffnen, wenn du nicht sicher bist.

Vorsicht bei Online-Shops: Nur vertrauenswürdige Anbieter nutzen, auf HTTPS und Bewertungen achten.

Achte bei Eingabe von Adress- und Zahlungsdaten unbedingt darauf, dass die URL mit **https://** (das "S" steht für Secure) beginnt und ein Schloss-Symbol  angezeigt wird. Nutze Plattformen wie [Trustpilot](#) oder [Rezensionen auf Google Maps](#), um die Seriosität des Shops zu prüfen. Auch ein Blick ins Impressum der jeweiligen Webseite ist wichtig.

Privates Umfeld einbeziehen: Auch Familie und Freunde sind Ziel von Betrügern – sprich mit ihnen darüber.

[Schockanrufe und der sogenannte "Enkeltrick"](#) betreffen zwar hauptsächlich Senioren, doch die Täter nutzen dafür oft gestohlene Daten jüngerer Verwandter. Je mehr alle Bescheid wissen, desto geringer ist die Chance, dass jemand auf solche Maschen hereinfällt.

Check deine Daten: Prüfe auf [Have I Been Pwned](https://haveibeenpwned.com/), ob deine E-Mail-Adresse oder Passwörter bereits in Datenleaks aufgetaucht sind.

Notfallplan kennen: Wenn etwas passiert, sofort handeln: **Trenne betroffene Geräte vom Internet, sichere Beweise und informiere bei Zahlungsbetrug deine Bank oder den Kreditkartenanbieter** (Sperrhotline für Karten und OnlineBanking: 116 116). [Auch das Bundesamt für Sicherheit in der Informationstechnik \(BSI\) steht für jeden kostenlos unter der 0800 274 1000 zur Verfügung.](https://www.bsi.de/bsi/deutschland/bsi-beratung/bsi-beratung-fuer-sicherheit/bsi-beratung-fuer-sicherheit-in-der-informationstechnik/bsi-beratung-fuer-sicherheit-in-der-informationstechnik.html) Bei größeren Vorfällen kann die Polizei hinzugezogen werden.

Die richtige Reaktion hängt immer vom Umfang und der Art des Angriffs ab.

Im Unternehmen gilt: Unverzüglich Vorgesetzten, IT oder die Informationssicherheit informieren.

Fazit

Cybersecurity ist kein IT-Thema, sondern eine Gemeinschaftsaufgabe. Jede und jeder von uns ist Teil der Verteidigungsline – privat und beruflich. **Die gute Nachricht: Mit Wissen, Wachsamkeit und konsequentlichem Handeln können wir die Risiken deutlich senken.**

Wpl-MaRisk kommt!



Die BaFin wird voraussichtlich im 1. Quartal 2026 die **Mindestanforderungen an das Risikomanagement von Wertpapierinstituten“ (Wpl-MaRisk)** veröffentlichen.

Diese werden den aufsichtlichen Rahmen des Wertpapierinstitutsgesetzes (WpIG) für kleine und mittlere Wertpapierinstitute konkretisieren. Wir unterstützen seit über 20 Jahren Sparkassen und andere

mittelgroße Finanzinstitute bei der Einhaltung der MaRisk (BA). Und natürlich verfolgen wir das aktuelle Konsultationsverfahren, das die BaFin für die Entwicklung der Wpl-MaRisk aktuell durchführt, sehr genau. Daher verfügen wir über die Expertise und Erfahrung, kleine und mittlere Wertpapierinstitute bei der Umsetzung wirkungsvoll und effizient unterstützen zu können - bereits jetzt mit **fundierte** **Experten-Einschätzungen**, und natürlich auch unmittelbar nach der Veröffentlichung des Rundschreibens mit **praxisnaher Hands-on-Unterstützung**.

Fit für Prävention von Geldwäsche und Terrorismusfinanzierung 2027

Wir unterstützen bei der Umsetzung des neuen EU-AML-Pakets - Banken und Sparkassen, aber auch Notare, Immobilienmakler, Juweliere, Kunsthändler, Händler hochwertiger Pkw etc. - schlichtweg alle künftig Verpflichteten.

Die Europäische Union hat mit dem AML-Paket (Anti Money Laundering) einen ambitionierten Rahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung verabschiedet. Ab 2027 tritt das Paket verbindlich in Kraft – mit weitreichenden Anforderungen an Compliance-Strukturen, Risikomanagement und interne Kontrollsysteme.



Nicht unter Zeitdruck geraten (“Das ist ja noch lange hin“). Jetzt schon mit der Vorbereitung beginnen, damit Sie entspannt, aber zielorientiert vorgehen können. Die neuen Anforderungen machen teilweise sehr umfangreiche Arbeiten notwendig. Das beginnt schon bei der Gap-Analyse, also beim Abgleichen Ihrer bestehenden Prozesse. Wir unterstützen Sie dabei, sich frühzeitig auf diese Änderungen vorzubereiten: Von der Analyse bestehender Prozesse über die Anpassung interner Richtlinien bis hin zur Schulung von Mitarbeitenden. So stellen Sie sicher, dass Ihre Organisation rechtzeitig konform ist und Risiken effektiv minimiert werden.

Jetzt handeln und 2027 fit sein – wir begleiten Sie Schritt für Schritt.

Risk in Focus 2026 des DIIR

Das [Deutsche Institut für Interne Revision e.V. \(DIIR\)](#) hatte Ende September die Ergebnisse seiner Befragung „[Risk in Focus 2026 -Hot Topics for Internal Auditors](#)“ veröffentlicht. Zentrale Erkenntnisse inkl. Raum für Diskussionen wurden in einem Webinar am 12. Dezember 2025 vorgestellt.

Als Top-Risiken und Herausforderungen für 2026 werden insbesondere gesehen:

- Cybersicherheit und Datensicherheit
- Humankapital und Talentmanagement
- Digitale Disruption und Künstliche Intelligenz
- Die makroökonomische und geopolitische Unsicherheit

Wir unterstützen Sie auch bei diesen Herausforderungen gern!

DORA-Informationsregister



Wir unterstützen Sie bei allen Engpässen...

In Zeiten knapper Ressourcen können kurzfristige Engpässe bei **der Erfassung noch fehlender Informationen oder der aufwändigen Aktualisierung des Informationsregisters** schnell zur Herausforderung werden. Die **ETL consit** steht Ihnen zur Seite, um diese Hürden gemeinsam zu überwinden.

Unsere Unterstützung für Ihr Institut:

- **Starkes Engagement:** Unser engagiertes Team ist bereit, Ihnen sofort und umfassend zu helfen, damit alle relevanten Informationen rechtzeitig und korrekt erfasst werden bzw. Engpässe so schnell wie möglich überwunden werden. Wir lassen Sie in schwierigen Situationen nicht allein!
- **Kompetente Unterstützung:** Unsere Spezialisten kennen alle gängigen Tools und Systeme. Mit Expertise und Erfahrung helfen wir Ihnen, die Anforderungen des Informationsregisters zu erfüllen und Verzögerungen zu vermeiden. Ihre Sorgen sind unsere Priorität.
- **Zuverlässigkeit:** Vertrauen Sie auf unsere bewährten Prozesse und Best-Practice-Lösungen. Wir sind Ihr verlässlicher Partner in jeder Situation.

Kontaktieren Sie uns noch heute! Erfahren Sie mehr über unsere Dienstleistungen und wie wir Sie bei der Bewältigung Ihrer Herausforderungen unterstützen können. **Gemeinsam sorgen wir dafür, dass Ihr Institut bestens aufgestellt ist.**

EU plant „Digital Omnibus“-Paket – Weniger Bürokratie, klarere Datenschutzregeln!

Die EU-Kommission hat ihr neues **Digital-Omnibus-Paket** vorgestellt – und für Unternehmen bringen die Vorschläge vor allem eines: **mehr Klarheit und weniger Komplexität**, besonders im **Datenschutz**.

Dabei sollen im Kern die Vorschriften des Data Governance Acts (Regulation (EU) 2022/868) mit den Vorschriften der Open Data-Richtlinie (Directive (EU) 2019/1024) und der Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (Regulation (EU) 2018/1807) in den Data Act integriert werden.



Was heißt das für den Datenschutz konkret?

Präzisere DSGVO-Begriffe

Die Definition *personenbezogener Daten* wird an die aktuelle EuGH-Rechtsprechung angepasst. Das schafft Rechtssicherheit – besonders beim Thema „relativer Personenbezug“.

Neue Rechtsgrundlage für KI & sensible Daten

Für die **Entwicklung von KI-Systemen** soll eine neue DSGVO-Grundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten kommen. Ein wichtiger Schritt, um Innovation und Datenschutz in Einklang zu bringen.

Einheitliche Meldestelle für Cybervorfälle

Statt Meldungen an BSI, BaFin & Co. soll es künftig **eine zentrale Meldestelle bei der ENISA** geben. So führt eine harmonisierte Anlaufstelle zu weniger Bürokratie und erleichtert die Einhaltung von Meldepflichten enorm – auch in Verbindung mit dem Cyber Resilience Act.

Schutz von Geschäftsgeheimnissen & Entlastung für KMU

Im Datenwirtschaftsrecht werden **Geschäftsgeheimnisse stärker geschützt** und **Datenschutz- & Compliance-Pflichten für kleinere Unternehmen weiter entschlackt**.

Was passiert als Nächstes?

Der Entwurf wurde am **19. November 2025** veröffentlicht und geht jetzt ins EU-Gesetzgebungsverfahren. Änderungen sind also noch möglich – aber die Richtung ist klar: **mehr Harmonisierung, weniger Bürokratie, stärkerer Datenschutzfokus**.

Unsere **Spezialisten** sind bei allen Fragen des Datenschutzes eng an Ihrer Seite!

Weihnachtsfeier der ETL consit in Hamburg mit Besuch des Miniatur-Wunderlands!

Die Weihnachtsfeier der ETL consit fand in diesem Jahr in Hamburg statt.

Nach einem stärkenden Abendessen im Restaurant „Heimathafen“ durften wir an einer beeindruckenden Abendführung im Miniatur Wunderland teilnehmen. Eine schöne und unglaublich faszinierende Veranstaltung!

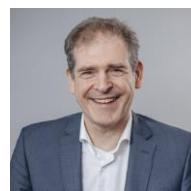


Ihre Ansprechpartner



Bernd Schmid
Geschäftsführer

Telefon (04531) 66 96-28
Mobil (0160) 90 17 50 68
bernd.schmid@etl-consit.de



Oliver Gose
Mitglied der Geschäftsführung

Telefon (04531) 66 96-422
Mobil (0162) 372 42 17
oliver.gose@etl-consit.de

ETL consit GmbH

Schützenstraße 25a
23843 Bad Oldesloe
Telefon (04531) 66 96-0
Fax (04531) 66 96-45
info@etl-consit.de
www.etl-consit.de