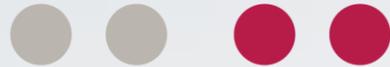


s | consit



Ihr Partner für Revision, Risikomanagement, Datenschutz,
Informationssicherheit, Compliance und Rechnungswesen.



Mitarbeitersensibilisierung Schutz vor Phishing und mehr...

ppa. Dipl. Inf. Sven Lammers

08.09.2022 | www.s-consit.de

MEMBER OF

ETL
GLOBAL

Kurzvorstellung s-consit GmbH



44

Mitarbeiter

340+

Mandanten

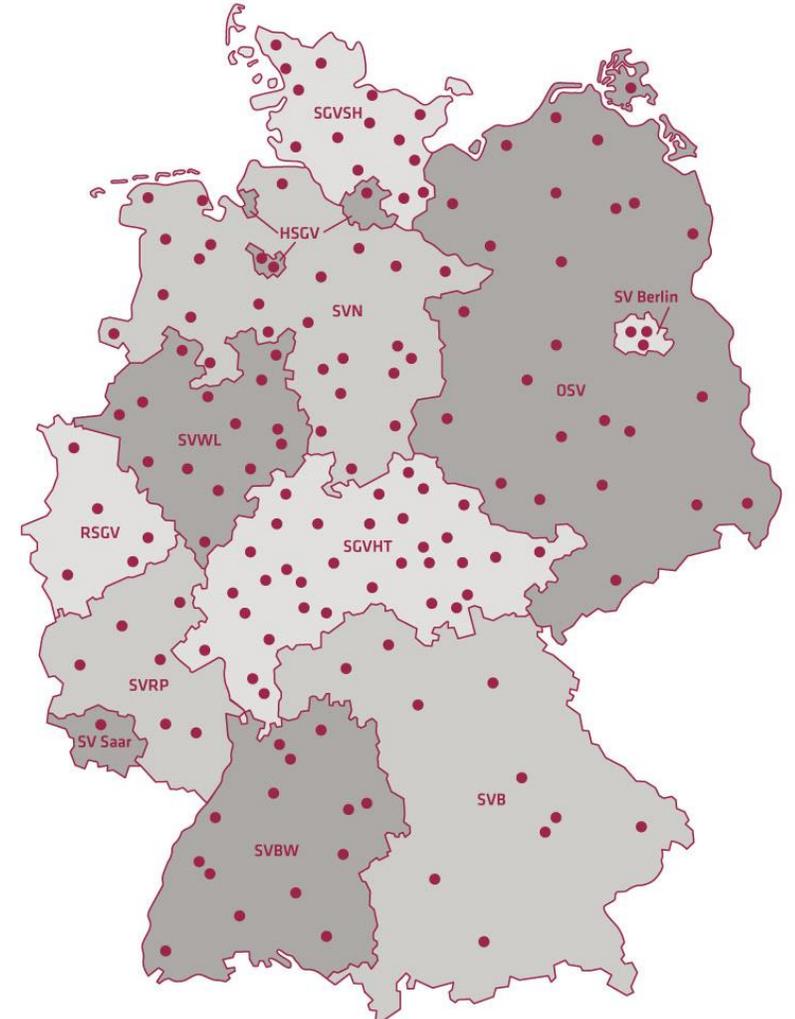
5400+

Prüfungs- und Beratungstage

Branchenfokus:

- Mittelstand verschiedener Branchen u.a. Software, IT, Agrarindustrie, Lebensmittelindustrie, Immobilien...
- Finanzdienstleister, darunter ca. 270 Sparkassen
- Banken & Finanzdienstleister

Seit 2020 besteht eine strategische Partnerschaft mit der ETL AG Wirtschaftsprüfungsgesellschaft.



Informationssicherheit und Datenschutz...

- ...sollen den Schutz von Informationen gewährleisten
- ...umfasst nicht nur technische, sondern auch organisatorische, infrastrukturelle und **personelle** Aspekte
- ...ist nicht nur Aufgabe von Experten, sondern auch **Aufgabe aller Mitarbeiter!**



144 MIO. **+ 22 %**
neue Schadprogramm-Varianten gegenüber 2020:
117,4 MIO.

DURCHSCHNITTLICH

394.000

2020: 322.000

neue
Schadprogramm-
Varianten pro Tag

IM HÖCHSTWERT

553.000

2020: 470.000

DOPPELT SO VIELE
BOT-INFESTIONEN DEUTSCHER SYSTEME
pro Tag im Tagesspitzenwert

20.000 **> 40.000**

98 %



aller geprüften Systeme waren durch
Schwachstellen in **MS Exchange** verwundbar.

Quelle: www.BSI „Lage der IT-Sicherheit 2021“

Warum Schulung & Sensibilisierung?

- Die Wirksamkeit technischer Sicherheitsmaßnahmen ist oft von der **korrekten Anwendung** organisatorischer Maßnahmen abhängig.
 - z.B. Nutzung von verschlüsselten E-Mails
- Firewalls, Virens Scanner und Webfilter helfen selten bei **menschlichen Fehlverhalten** und Informationsverlusten.
 - z.B. falsche Sicherheitseinstellungen, versehentliches Veröffentlichen oder Öffnen von schädlichen Dokumenten
- Nur **bekannte Vorgaben und Richtlinien** können eingehalten werden.



Ziel: Schaffung von Sicherheitsbewusstsein

Fähigkeit, Sicherheitsbedrohungen, Schutzbedarf und Risiken korrekt einzuschätzen.



Unfallfoto von Rosar aus den Stuttgarter Nachrichten

Sicherheitsbewusstsein aller Mitarbeiter, Führungskräfte und Vertragspartner ist der wichtigste Faktor:

- Nicht nur Kenntnis, sondern **verstehen** von Sicherheitsmaßnahmen.
- Mitarbeiter müssen
 - wissen was von ihnen erwartet wird.
 - sich der Sicherheitsbedrohungen bewusst sein.
 - die Ursachen für Sicherheitsvorfälle kennen und vermeiden.
 - sich verantwortlich fühlen und sich ihrer persönlichen Rolle bewusst sein.

„Menschliche Firewall“



„Phishing“

- Unter **Phishing** werden Versuche verstanden, über gefälschte WWW-Adressen, E-Mail oder Kurznachrichten an Daten eines Internet-Benutzers zu gelangen und damit **Identitätsdiebstahl** zu begehen um mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden.
- Es handelt sich meist um kriminelle Handlungen, die Techniken des Social Engineering verwenden:
 - Phisher geben sich als vertrauenswürdige Personen aus.
 - Phishing-Nachrichten werden meist per E-Mail oder Instant-Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben.
 - Typisch ist dabei die Nachahmung des Designs einer vertrauenswürdigen Stelle

Beo



Sparkasse

Web-Seite
S-CERT

bit

**Sie haben sich erfolgreich angemeldet. Vielen Dank für Ihre Anmeldung.
Aufgrund einer hohen Auslastung steht das Online-Banking derzeit leider nicht zur Verfügung.**

Wir bitten um Ihr Verständnis.

- Privatkunden
- Firmenkunden
- Private Banking
- Ratgeber
- Ihre Sparkasse
- Service/Kontakt

Online-Banking ist ganz einfach!

Mit Online-Banking wissen Sie immer was auf Ihren Konten los ist. Egal, ob Sie zu Hause sind oder unterwegs, sogar im Urlaub.

[Online-Banking freischalten](#)

- Vorteile
- So geht's
- Hilfreiche Tipps
- FAQ

Home > Online- und Mobile-Banking

Bankgeschäfte so einfach wie möglich machen

Diese Herausforderungen kennt wohl jeder:

- ✓ Den Kontostand im Blick behalten
- ✓ Auf den letzten Drücker etwas bezahlen müssen
- ✓ Einen Kontoauszug oder eine bestimmte Buchung finden, z.B. für die Steuererklärung

Mit Online-Banking ist das alles kein Problem: Jederzeit, von (fast) jedem Ort - und immer sicher und zuverlässig.

Demokonto ausprobieren

Bedrohungen



Meine Sicherheit | Mein Konto | Amazon.de

Sicherheitsmeldung

E-Mail Referenz: #028-3371852-3321807

Merkmale einer Phishing-Mail

- Unpersönliche Anrede
- Drohung & Dringlichkeit

Sehr geehrte/r Kunde/in,

bei Ihrem Amazon-Konto wurden verdächtige aktivitäten festgestellt. Wir bei Amazon nehmen die Kunden-Sicherheit äußerst ernst. Aus Sicherheitsgründen müssen Sie bei Ihrem Nutzerkonto Ihre persönlichen Daten bestätigen. Bis dahin wurde Ihr Nutzerkonto eingeschränkt.

Diese Sicherheitsmaßnahme schützt Sie vor Missbrauch durch Dritte.

Bei der Bestätigung müssen Sie alle nötigen Informationen zu Ihrem Nutzerkonto und Zahlungsdaten eintragen, da Sie sonst nicht mehr in der Lage sind, weitere einkäufe durchzuführen.

Klicken Sie auf den unten angezeigten Link und folgen Sie den Anweisungen.

Wird festgestellt, dass Sie falsche Informationen / falsche Zahlungsdaten eingeben oder diese Bestätigung ignorieren, wird Ihr Nutzerkonto vollständig gesperrt und Sie an unsere Sicherheitsabteilung gemeldet.

[Weiter \(über den Sicherheitsserver\)](#)

Quelle: pcwelt.de

- Gefälschter Link (erkennbar über Mouse-Over)

Warnhinweis der Münchner Polizei vom 01.09.2022

Die Polizei München warnt vor der Betrugsmasche des sogenannten „**CEO-Fraud**“. Unbekannte Täter geben sich, nach Sammlung jeglicher Art von Information über das anzugreifende Unternehmen, als Geschäftsführer (CEO) des Unternehmens aus und veranlassen eine Mitarbeiterin/einen Mitarbeiter zum Transfer eines größeren Geldbetrages auf in- oder ausländische Konten.

Die Kontaktaufnahme erfolgt in der Regel über E-Mail. Diese wird durch den Täter verfälscht, sodass sie beim Mitarbeiter des Unternehmens den Eindruck erweckt, als würde es sich um den CEO des Unternehmens handeln. Durch teils geschickten Einsatz der folgenden Faktoren gelangen die Täter so immer noch an teils erhebliche Geldbeträge:

- Bezugnahme auf vorherige Kommunikation
- Einsatz von angeblichen Zeitdruck und Dringlichkeit
- Herausstellen der Wichtigkeit des angeschriebenen Mitarbeiters
- Begründung der Vertraulichkeit innerhalb des Unternehmens
- Autorität und Befugnis des vermeintlichen CEO werden eingesetzt





Zutritt Unberechtigter

Ziele:

- Diebstahl von Informationen und Sachwerten.
- Installation von Keyloggern und Schadsoftware.

Seien Sie wachsam!! Die Angreifer sind kreativ:

- Ich bin der neue Kollege / Auszubildende / Praktikant ...
- Ich habe mich verirrt, wo finde ich ...
- Zutritt als Servicetechniker, Pizzabote, nette Besucherin mit zwei Kaffeetassen in der Hand
- Kündigen sich selber per E-Mail / Telefonanruf / Fax an.
- Nutzen gefälschte Ausweise mit offiziellen Logos.



**Geschäftsführung setzt
sichtbare Zeichen**



Nachhaltigkeit & Aktualität

Gesamtheitliches abgestimmtes Konzept

Schulen

Wissen vermitteln

&

regelmäßig **Sensibilisieren**

Sicherheitsbewusstsein aufrecht erhalten



Persönlichen & privaten Nutzen aufzeigen

PIN:
1234

Passwort:
admin

Umsetzung in der Praxis

- Präsenzs Schulung / Webinare
- Web Based Trainings
- Wissenstests / Gewinnspiele
- Intranetbeiträge
- Newsletter
- Flyer / Poster
- Phishingtests

- Messung von Sicherheitsbewusstsein und -wissen



**IT-Sicherheit.
Made in Holstein.**

 **Sparkasse
Holstein**

Umsetzung in der Praxis



INHALTSVERZEICHNIS

- 1 Regel 1 – Aufbau eines notwendigen Basiswissens
- 2 Regel 2 – Installieren Sie Updates und verwenden Sie nur aktuelle Software
- 3 Regel 3 – Surfen Sie niemals
- 4 Regel 4 – Setzen Sie professionell ein
- 5 Regel 5 – Verwenden Sie immer eine Firewall und eine Antivirenschutzsoftware
- 6 Regel 6 – Wählen Sie den richtigen Browser
- 7 Regel 7 – Verwenden Sie sichere Kennwörter
- 8 Regel 8 – Verhalten Sie sich professionell
- 9 Regel 9 – Achtung bei E-Mails
- 10 Regel 10 – Erstellen Sie regelmäßig Backups Ihrer Daten

11 Checkliste zu den 10 Regeln
12 Schlusswort

1. Aufbau eines notwendigen Basiswissens

Um sich als Autofahrer sicher im Straßenverkehr zu bewegen, benötigen Sie neben einem sicheren Fahrer...

7. Verwenden Sie sichere Kennwörter

Hacker verfügen über hunderte von Möglichkeiten, um Kennwörter zu hacken. Angefangen bei spezialisierten Programmen, mit denen vollautomatisch alle möglichen Zeichenfolgen oder Wörterbücher kombiniert mit Zahlen getestet werden, bis zu Programmen, mit welchen Kennwörter einfach mitgelesen werden können. Damit Sie sich vor solchen Angriffen schützen können, müssen Ihre Kennwörter spezielle Sicherheitsanforderungen erfüllen.

Sicherheitsanforderungen an Ihre Kennwörter:

Verwenden Sie bei jedem Internetanbieter ein anderes Kennwort

Sie werden sich sicherlich fragen, warum Sie nicht ein Kennwort für unterschiedliche Internetanbieter nehmen sollen. Nahezu täglich werden Internetanbieter von Kriminellen gehackt und die Zugangsdaten (beispielsweise E-Mail-Adresse und Kennwörter) gestohlen. Mit diesen Identitätsdaten versuchen Kriminelle, sich dann bei anderen Internetdienstleistern anzumelden und zum Beispiel mit der gestohlenen Identität Waren zu bestellen.

Langes Kennwort

- Ihr sicheres Kennwort ist mindestens 10 Zeichen lang (WPA/WPA2-Kennwörter mindestens 30 Zeichen) und besteht aus kleinen Buchstaben, großen Buchstaben, Zahlen und Sonderzeichen, also beispielsweise `1fj$&SmmF20kddPW!`.
- Es kommt nicht in Wörterbüchern vor. Auch und insbesondere sind Namen der Familienmitglieder, des Haustiers, von Freunden, von Prominenten, Geburtsdaten, Kfz-Kennzeichen etc. tabu.
- Es besteht nicht aus Tastaturfolgen wie beispielsweise: `1234qwert!""$$`
- Einige Internetanbieter geben bei der Anmeldung oder bei der Kennwortänderung Kennwörter vor; diese bitte umgehend ändern.
- Geben Sie niemals Ihr Kennwort an jemanden weiter, auch nicht wenn Sie per Telefon, E-Mail oder auf Websites danach gefragt werden.
- Ändern Sie Ihre Kennwörter regelmäßig, zumindest zweimal im Jahr.

Quelle: Sparkasse Münsterland Ost

Umsetzung in der Praxis

Mailboxgröße überschritten

max.mustermann@musterfirma.de
An Lammers, Sven

Email account quota configuration settings for [sven.lammers@consit.de](#)

| | |
|------------------|--|
| E-Mail-Adress: | sven.lammers@consit.de |
| Incoming Server: | IMAP Port POP3 Port |
| Outgoing Server: | SMTP Port |
| Mailbox Size: | 207 MB |

[Bitte klicken Sie hier, um Ihr Postfach zu erweitern](#)

This is an automated message, do not reply.

Hallo von Marion Müller - Nachricht (HTML)

Hallo von Marion Müller

max.mustermann@musterfirma.de
An Lammers, Sven

So 29.08.2021 16:56

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

LinkedIn

Hallo,
Marion Müller hat Sie vor 6 Tagen eingeladen, sich auf LinkedIn zu vernetzen.



Marion Müller
Immobilienmanagerin an der Hochschule für Angewandte Wissenschaften Hamburg (HAW Hamburg)

[Einladung annehmen](#)

[Abbestellen](#) | [Hilfe](#)

Ihre E-Mail-Adresse wird in Funktionen wie "Personen, die Sie vielleicht kennen" verwendet, um Kontaktvorschläge zu machen.

Diese E-Mail wurde an [sven.lammers@s-consit.de](#) gesendet.

LinkedIn

(C) 2021 LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Irland. LinkedIn ist eingetragener Firmenname der LinkedIn Ireland Unlimited Company. LinkedIn und das LinkedIn Logo sind eingetragene Marken von LinkedIn.

Videos und mehr

- BSI #einfachaBSIchern
 - Erläuternder Text
 - Video
 - Klickbare Grafik

- <https://www.einfachabsichern.de>
- <https://www.digital-kompass.de>



Umsetzung in der Praxis

Guerilla-Marketing



Quelle: <http://www.besser-ausgebildet.de/>



Ansprechpartner der s-consit GmbH



Sven Lammers
Bereichsleiter Beratung,
Prokurist
04531 6696-25
sven.lammers@s-consit.de



Bernd Schmid
Bereichsleiter Vertrieb,
Prokurist
04531 6696-28
bernd.schmid@s-consit.de



Sven Bethke
Bereichsleiter Revision,
Prokurist
04531 6696-20
sven.bethke@s-consit.de



Vielen Dank!