

kaspersky

# Kaspersky – aktuelle Bedrohungsszenarien

Stefan Zysset / *Senior Presales Engineer* / [stefan.zysset@kaspersky.com](mailto:stefan.zysset@kaspersky.com)

Michael Zeger / *Territory Manager Austria* / [michael.zeger@kaspersky.com](mailto:michael.zeger@kaspersky.com)

# Brand bei Europas größtem Cloudanbieter OVH betraf 3,6 Millionen Webseiten

Viele Kunden ohne Backup, große Datenmengen zerstört – auch einige Sicherungen betroffen

14. März 2021, 17:38 366 Postings



Foto: AFP/Sapeurs-pompiers du Bas-Rhin

<https://www.derstandard.at/story/2000125032535/brand-bei-europas-groesstem-cloudanbieter-ovh-betraef-3-6-millionen?ref=rec>

kaspersky



Webinar "Microsoft Exchange Server Zero-Day-Exploits - was ist jetzt zu tun?"

# Das Problem

## Menschen sind das schwächste Glied in der Cybersicherheit

**52%** der Unternehmen betrachten Mitarbeiter als die größte Bedrohung für die Cybersicherheit \*

**60%** der Mitarbeiter haben vertrauliche Daten auf ihrem Unternehmensgerät (Finanzdaten, E-Mail-DB usw.) \*\*



**30%** der Mitarbeiter geben zu, dass sie die Anmelde- und Kennwortdaten ihres Arbeits-PCs mit Kollegen teilen \*\*

**23%** der Organisationen haben keine Cybersicherheits-Regeln oder -Policies für die Speicherung von Unternehmensdaten \*\*

## Ist es in letzter Zeit sicherer geworden?

**50%**

Unternehmen, die das Arbeiten von persönlichen Geräten erlauben, haben keine Richtlinien, wie diese genutzt werden sollen

**32%**

Unternehmen stellen ihren Mitarbeitern AV-Programme zur Verfügung, die sie auf privaten Geräten zu Arbeitszwecken nutzen können

**27%**

Mitarbeiter erhielten bösartige E-Mails, die CORONA/COVID-19 als Hauptthema verwenden

**53%**

verwenden ein VPN, wenn Sie von zu Hause aus arbeiten

**51%**

Arbeitnehmer geben zu, dass sie „Inhalte für Erwachsene“ auf Geräten ansehen, die sie für die Arbeit nutzen

**73%**

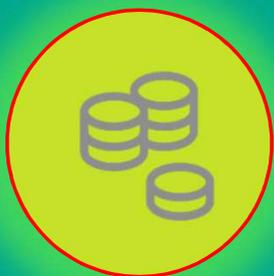
Mitarbeiter haben seit der Umstellung auf WFH (Home Office), KEIN IT Security Awareness-Training erhalten

*"How COVID-19 changed the way people work". Kaspersky, April 2020, based on 6,017 respondents survey in the UK, USA, Australia, France, Italy, Spain, Germany, Sweden, Russia, Mexico, Brazil, Colombia*



# Menschliches Versagen als Cyber-Risiko für das Unternehmen

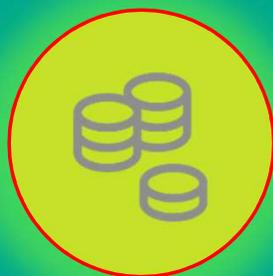
Das Verhalten der Mitarbeiter ist ein großes IT-Sicherheitsrisiko, auch wenn evtl. traditionelle Awareness-Programme vorhanden sind:



**\$1,057,000**

pro Enterprise Organisation

The average financial impact of **data breaches** caused by inappropriate IT resource use by employees \*



**\$98,000**

pro SMB

The average financial impact of **data breaches** caused by inappropriate IT resource use by employees \*

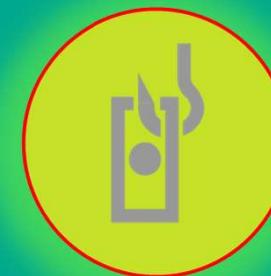


**\$101,000**

pro SMB

The financial impact of attacks caused by **phishing/social engineering\***

(\$1,3M per enterprise) \*\*



bis zu **\$400**

pro Mitarbeiter pro Jahr

The average cost of **phishing attacks** alone\*\*\*

\* Report: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives". Kaspersky Lab, 2019

\*\* Report: "Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", Kaspersky Lab and B2B International, June 2017.

\*\* Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.

kaspersky

# Automated Security Awareness Platform (ASAP)

# Herausforderungen bzgl. Security-Awareness...

## Nicht effizient für die Mitarbeiter:



wird als schwierig, langweilig und irrelevant empfunden.



es geht eher um "Verbote" als um das "Wie"



Wissen bleibt nicht erhalten



Lesen und Hören ist nicht so effizient wie das „Tun“

## Herausforderungen für Admins (z.B. SMB)



Wie erstelle ich ein Programm und setze Ziele ?...



Wie verwalte ich Training-Assignments ?...



Wie kann man den Fortschritt kontrollieren ?...



Wie kann man Menschen in ein Training einbeziehen ?...

# ASAP – Überblick

**ASAP** = ideal für Unternehmen, die sofort starten möchten mit voll automatisierten, einfachen Management und festgelegten Trainings

- integrierte Plattform für Schulung, Assessments, Simulierte Phishing-Angriffe und Reporting
- **SaaS/Cloud Plattform** (auch als **SCORM Module**)
- **17 Sprachen** (Engl. Dt. Fr. It. SpEU. SPLat. Port. Rus. Arab. Poln. Tschech. Türk. Slov. usw. )
- „Automated Micro-Learning Path“
- **Standalone Phishing Simulator** (seit 29.07.20 )
  
- **MSP Unterstützung**
- **VSMB und SMB Ready** (ab 5+ Benutzer)
- **Monatliche Subscription** (bei SaaS/Cloud)



Schulungs-  
module

+

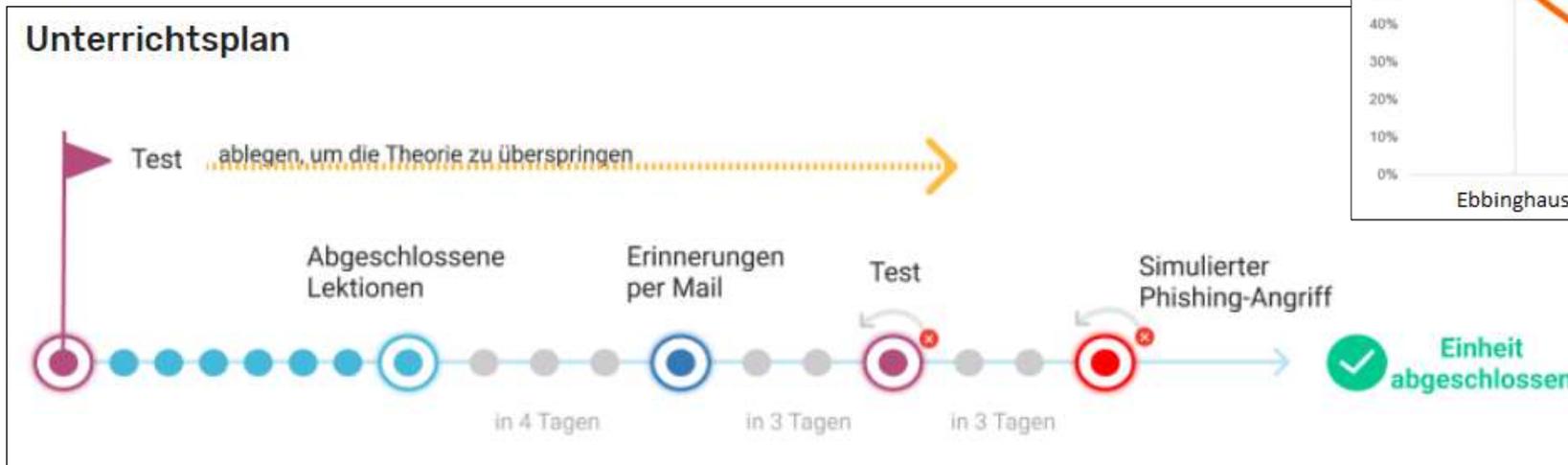
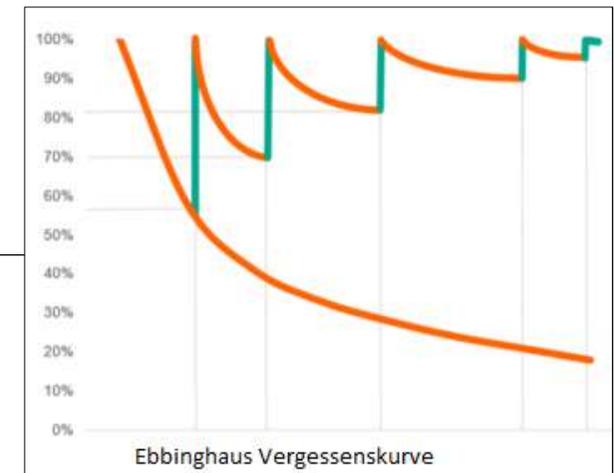
Simulierte Phishing-  
Angriffe

Skills  
Assessment

Analyse und Reporting

# ASAP

- Voll-Automatisiertes Learning-Management in 4 Schritten
- 4 Level (aktuell 3) pro Trainings-Modul d.h. *Anfänger, Grundlagen, Fortgeschritten* und zukünftig *Advanced*
- „*Micro Learning*“ – Inhalte sind speziell konzipiert (2 bis 15 Minuten), um langweilige und langwierige Lektionen zu vermeiden



# ASAP

ASAP erstellt automatisch einen Zeitplan – basierend auf dem gewünschten Qualifikations-Niveau und dem Lerntempo

**GRUPPE LOW RISK** Trainingsplan Statistiken

**Anfänger**  
Zielniveau

**30**  
Intensität  
(Minuten pro Woche)

**3**  
Gesamtstunden

**2**  
Anzahl der Nutzer

**ZEITPLAN DES TRAININGS**

Thema	Startzeitpunkt	Endzeitpunkt
Einführung i...	Nov 2018	Nov 2018
Passwörter u...	Nov 2018	Nov 2018
E-Mail	Nov 2018	Nov 2018
Web-browsing	Nov 2018	Nov 2018
Soziale Netz...	Nov 2018	Nov 2018
PC-Sicherheit	Nov 2018	Nov 2018
Mobile Geräte	Nov 2018	Nov 2018
Ergebnisse d...	Nov 2018	Nov 2018

**Gruppe bearbeiten**

Gruppenname \*  
Low Risk

Zielniveau  
Anfänger Grundlagen Intermediate

Intensität (Minuten pro Woche)  
10 20 30 ∞

**Achtung!** In dieser Gruppe werden bereits Schulungen durchgeführt, daher wirken sich Änderungen auf den Zeitplan aus. Sollen die Gruppenmitglieder gewarnt werden?

Nutzern eine E-Mail über Änderungen senden

Abbrechen Senden

# ASAP

Verschiedene Trainings-Elemente ergänzen sich gegenseitig, um die Awareness-Fähigkeit zu entwickeln

## INTERACTIVE LESSONS

### WHAT COULD HAPPEN IF MY PASSWORD IS TOO EASY OR IF I FORGET IT?

If your password isn't complex enough, it is easy to crack it. Once scammers can access your work or personal resources, they can carry out all sorts of acts on your behalf.

Press + for more information



Put materials on your social media accounts, like what happened to Mark Zuckerberg's Twitter

BACK NEXT

Kaspersky | ASAP



## TEST

10:32 k-asap.eu

2 من 15

### حدد الإجابة الصحيحة واضغط على "إجابة"

عرف مجرمو الإنترنت كلمة مرورك لمترجم حيوانات أليفة على الإنترنت، ولكنك لم تستخدمه لمدة عام على الأقل، ولا تعترم استخدامه مجددًا. ما الإجراء الواجب اتخاذه؟

- بتعين عليّ تغيير كلمة مروري وإبلاغ المختصين المسؤولين عن أمن شركتي بالواقعة.
- لا يلزمي فعل أي شيء. اقتحم مجرمو الإنترنت حسابي الشخصي الذي لا أستخدامه، لذا فهو لا تمثل تهديدًا لشركتي. وإذا حدث أي شيء، يمكنني إنشاء حساب جديد في المترجم على الإنترنت.

إجابة



## REINFORCEMENT

INCOMING

Subject: Properly storing your passwords is one of the most important parts of information security.  
From: ASAP  
To: user@company name.com

You should never use the same passwords for your work and personal accounts



## PHISHING SIMULATOR



Hello John!

You have registered a new account with Dropbox. If this was you, change your temporary password to a permanent one by following the link:

[Reset your password](#)

If you don't want to change your password, or if this request was made by someone else, immediately go to the [Security Center](#) and cancel the action: scammers could be acting on your behalf.

Please do not forward this message to anyone, otherwise your account security could be put at risk. In our help center, you will find [detailed security information](#).

Use with ease!

# ASAP

- Regelmäßige Benachrichtigungen z.B. via Mail, sind Teil der internen Kommunikation.
- Für jedes erlernte Thema bekommt der Student nun ein Zertifikat (nicht mehr nur pro Level)

**WEEKLY REMINDERS**

Your weekly report on program "The Basics of Cybersecurity"

Greetings, Moly!

This email contains your weekly report on the training

Planned completion date:  
**05.11.2019**

Estimated completion date: 17.01.2020

**Delay**  
In order to study at a comfortable pace and to complete the program on time, we recommend studying regularly, completing incomplete lessons, and proceeding to the next units without waiting for an invitation email.

Below are the recommendations for the modules of the program:

Introduction: Beginner
Email: Beginner

Expect the email notification about the availability of the next unit within a few days and immediately take it.

As soon as you catch up, try to keep up with the planned module completion dates and keep studying at the scheduled pace.

[Go to training](#)

**ADMIN'S REPORTS**

Status: training report on the program The Basics of Cybersecurity.

Hello, NFR Account!

This email contains a regular report on Status employees' training in the program The Basics of Cybersecurity. It includes key indicators, a link to the full training report, and a link to recommendations for further work with different employee groups, depending on their current training results.

Key indicators:

Progress	Employees	Recommendation
Ahead of schedule	0	-
Going well	1	Thank them. See <a href="#">Recommendations</a> .
Behind schedule	7	Provide additional motivation to continue training. See <a href="#">Recommendations</a> .
Significantly behind schedule	0	-
Can't finish on time	3	Perhaps you need to take advantage of additional organizational measures to engage your employees in training. See <a href="#">Recommendations</a> .
total	11	-

[View full training report](#)

**INVITATIONS**

Welcome to the education program

Dear Kitty,

NFR Account ([elena-mg+nfr@yandex.ru](mailto:elena-mg+nfr@yandex.ru)) has added you ([elena-mg+kitty@ya.eu](mailto:elena-mg+kitty@ya.eu)) to the list of students enrolled in the education program "The Basics of Cybersecurity", run by Locomotive.

To start learning, go to your [student portal](#), and confirm your agreement to learn.

We will also ask you to accept the education program privacy policy.

[START LEARNING](#)

If you think you got this message by mistake, please report it to [elena-mg+nfr@yandex.ru](mailto:elena-mg+nfr@yandex.ru).

If you have any questions related to the course, please don't hesitate to ask: [elena-mg+nfr@yandex.ru](mailto:elena-mg+nfr@yandex.ru)

Stay Aware!

**kaspersky**

**Certificate**

Le présent certificat d'achèvement du module «E-mail : Débutant» confirme que

**Bonaparte Napoleon**

à la suite de sa formation réussie au programme «Les principes fondamentaux de la cybersécurité», est capable de mettre en application des techniques permettant d'utiliser les messageries électroniques personnelles et professionnelles en toute sécurité, notamment en créant des mots de passe complexes et en contrant efficacement la fraude sur Internet.

26/08/2019

Les principes de base de la cybersécurité  
<https://k-asap.eu>



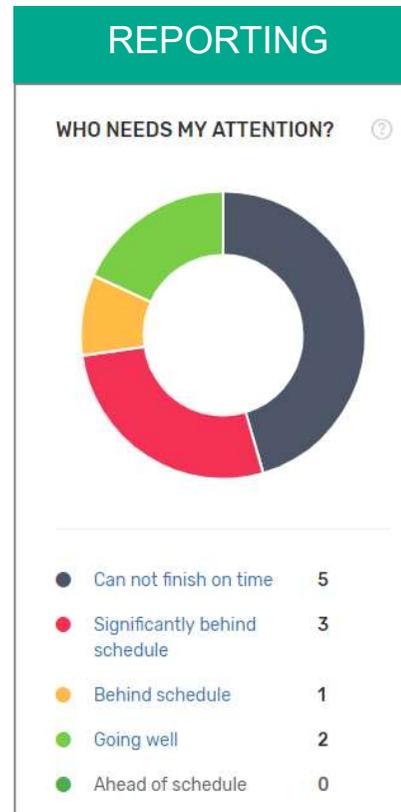
# ASAP – Admin-GUI

- Klares All-in-One Dashboard
- Alles notwendige auf einer Seite, was Sie benötigen – aktuell in 17 Sprachen

### ROUTINE TASKS

MY ACTIONS ?

- Add new users
- Import Users
- Start Group Training
- Add to training
- Pause Training
- Resume Training
- Download report



### LICENSE CONTROL

USERS & LICENSES ?

Studying	14
Completed	0
Unassigned	130
Paused	3
Total users	147

**10** Total number of available licenses

**30** Total number of licenses

# ASAP – Flexibler „Learning Path“

Für jede Trainings-Gruppe kann nun ausgewählt werden:

- Themen, welche die Studenten lernen müssen oder die ggf. übersprungen werden
- Ziel-Niveau, welches die Studenten für jedes bestimmte Thema erreichen sollen

Keine festen Zeit-Vorgaben mehr zwischen den Levels

- vorher Wartezeit von 7 Tage nach Abschluss der Anfänger-Stufe bis die nächste Stufe (Grundlagen) verfügbar war
- Rückstand kann nun schneller aufgeholt werden
- Simulierte Phishing-Angriffe (innerhalb des Lernfpads) wird nun zufällig über den Tag verteilt

Gruppe bearbeiten

Gruppenname \*  
Geringes Risiko

Intensität (Minuten pro Woche)  
10 20 30 ∞

Thema	Anfänger	Grundlagen	Intermediate
<input checked="" type="checkbox"/> Passwörter und Konten	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> E-Mail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Web-browsing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Soziale Netzwerke & Messenger	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> PC-Sicherheit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Mobile Geräte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**!** Achtung! In dieser Gruppe werden bereits Schulungen durchgeführt, daher wirken sich Änderungen auf den Zeitplan aus. Sollen die Gruppenmitglieder gewarnt werden?  
 Nutzern eine E-Mail über Änderungen senden

Abbrechen Senden

# ASAP – Admin – 4 Rollen

**ADMINISTRATOREN**

Hier können Sie neue Administratoren hinzufügen und deren Befugnisse bestimmen.

- **Hauptadministrator:** Verwaltet das Konto, die Administratoren, die Unternehmen
- **Unternehmensadministrator:** Verwaltet das Unternehmen und die im Unternehmen Kollegen im Unternehmen bestimmen.
- **Schulungsmanager:** Verwaltet die Schulungen im eigenen Unternehmen. Hat
- **Beobachter:** Kann nur die Trainingsparameter einsehen. Hat Zugriff auf einzel

Wählen Sie beim Hinzufügen von Administratoren die Sprache aus, in der die Einladung Administratorportal an sie gesendet werden soll.

Search

Name	E-Mail	Status	Hauptadminis...	Unternehmen	Unternehmen	Unternehmensadministrator	Schulungsmanager	Beobachter
Michael Hirschma	michael.hirschma	Aktiv	✓	MH-Company	✓	✓	✓	✓
				MH-Firma2	✓	✓	✓	✓
				MH-Firma3	✓	✓	✓	✓

### Administratorrechte

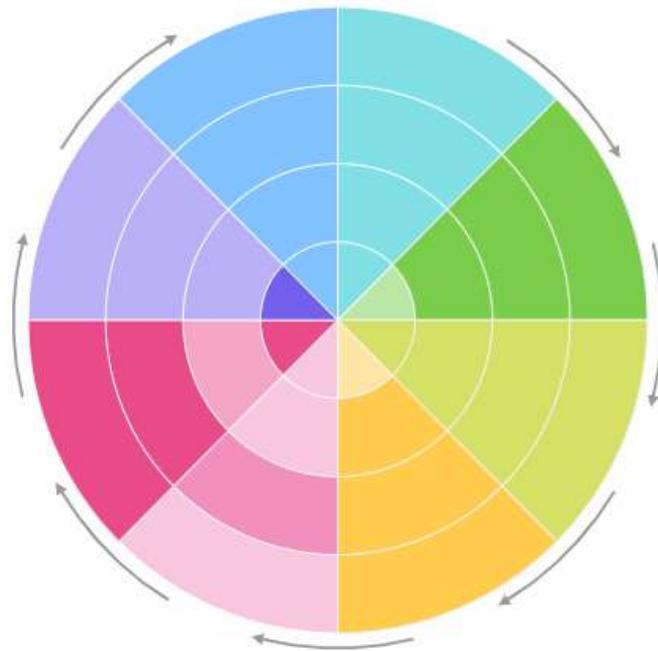
Hauptadministrator

Unternehmen	Unternehmensadministrator	Schulungsmanager	Beobachter
MH-Firma2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MH-Firma3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Abbruch

# ASAP – Admin/Benutzer – Modul-Überblick

LERNPLAN SECURITY AWARENESS



- Passwörter und Konten
- E-Mail
- Web-browsing
- Soziale Netzwerke & Messenger
- PC-Sicherheit
- Mobile Geräte
- Schutz vertraulicher Daten
- DSGVO

Über das Programm    Über Ebenen    Über Hashtags

Einige Aspekte der Cybersicherheit erfordern Kenntnisse und Fähigkeiten aus verschiedenen Bereichen und zu verschiedenen Themen. Hashtags zeigen, wo diese Fähigkeiten erlernt werden können.

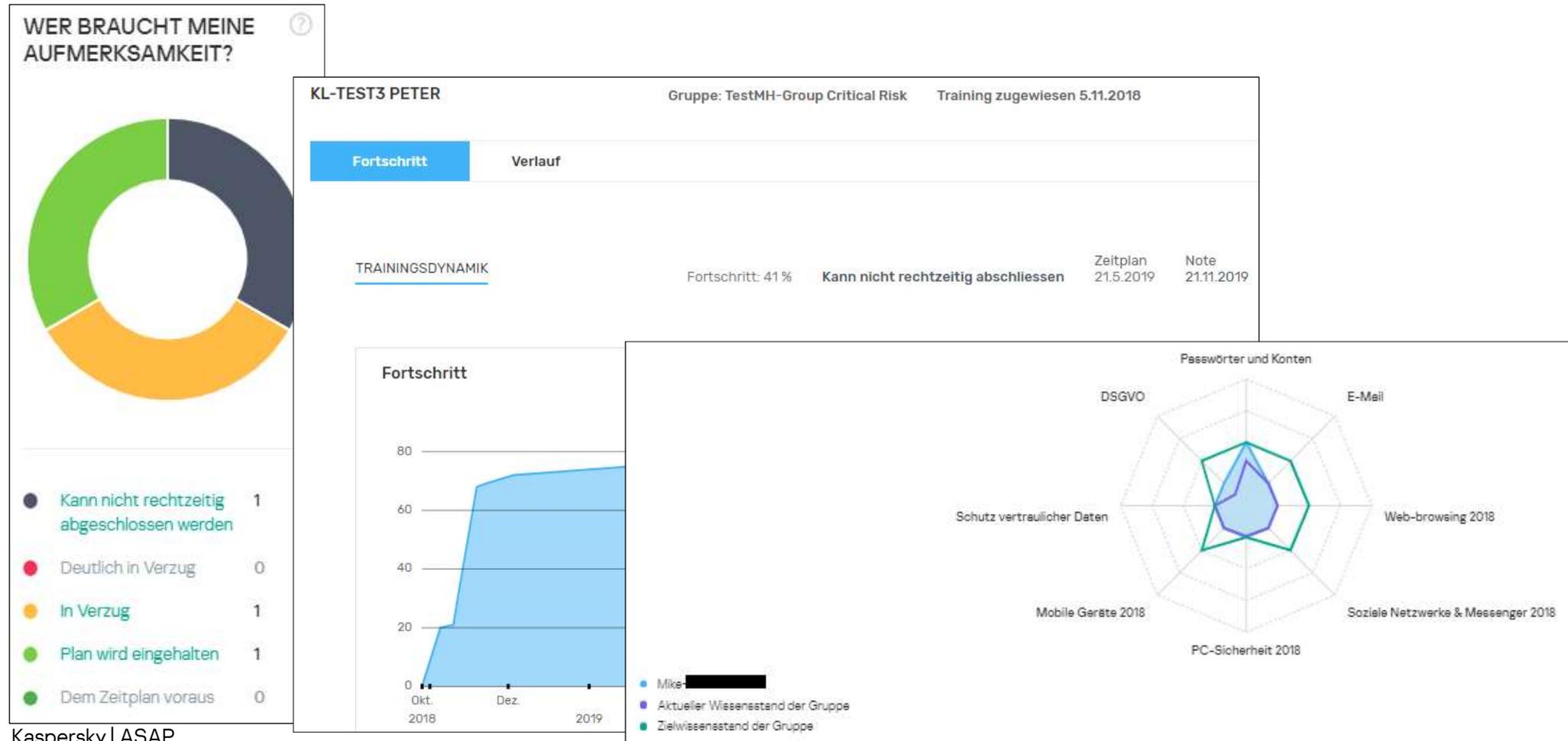
Drücken Sie auf den Hashtag, um die Module zu sehen, in denen solche Aspekte unterrichtet werden.

[#Passwörter](#)   [#Phishing](#)   [#GefährlicheLinks](#)   [#Ransomware](#)  
[#GefährlicheDateien](#)   [#Anwendungen](#)   [#SocialEngineering](#)



Social Engineering-Tricks können von Cyberkriminellen über mehrere Kommunikationskanäle (online und offline) angewandt werden. Nutzer müssen imstande sein, Merkmale der Manipulation in unterschiedlichsten Zusammenhängen zu erkennen.

# ASAP – Admin – Detaillierte Reports



# ASAP – Admin – Widerruf von Zertifikaten

**Aktionen**

- In Gruppe verschieben ...
- Training anhalten
- Training unterbrechen
- Schulung fortsetzen / zuweisen
- Archivierung
- Aus Archiv wiederherstellen
- Entfernen
- Zertifikate zurückziehen**

Olivia-3 Musterfrau kasperskyt

### Zertifikate zurückziehen

Bitte wählen Sie die Themen und Stufen, für die die Zertifikate der ausgewählten Benutzer zurückgezogen werden sollen.

**Thema \***

Passwörter und Konten 2018

**Stufe \***

- Intermediate**  Das Zertifikat wird zurückgezogen.
- Grundlagen**  Das Zertifikat wird zurückgezogen.
- Anfänger**  Das Zertifikat wird gespeichert.
- Die Zertifikate für alle Stufen werden zurückgezogen.

1 of 2 users will be affected, 1 certificate will be revoked.

**Kommentar**

Kommentar

Das Modul, für das das Zertifikat zurückgezogen wurde, wird automatisch neu zugewiesen, wenn es zum Schulungsprogramm für eine Benutzergruppe gehört.

Benutzer über Änderungen im Schulungsprogramm benachrichtigen

Diese Aktion kann nicht rückgängig gemacht werden.

# ASAP – Benutzer – Willkommen- und Training-Mail



Willkommen zum Trainingsprogramm

---



Sehr geehrte Peter,

Michael Hirschmann [REDACTED] hat Sie [REDACTED] auf die Liste der Teilnehmer am Schulungsprogramm Grundlagen der Cybersicherheit von MH-Company gesetzt.

Um mit dem Lernprogramm zu beginnen, gehen Sie bitte auf Ihr [Teilnehmerportal](#) und bestätigen Sie Ihre Zustimmung zum Lernprogramm. Wir bitten Sie außerdem darum, die Datenschutzrichtlinie des Trainingsprogramms zu akzeptieren.

[LERNPROGRAMM BEGINNEN](#)

---

Wenn Sie der Meinung sind, dass Sie diese Nachricht versehentlich erhalten haben, schicken Sie bitte eine Meldung an [REDACTED].



Wir laden Sie ein, sich mit dem Trainingsmodul "Passwörter und Konten: Anfänger" des Programms "Grundlagen der Cybersicherheit" zu beschäftigen.

---



Hallo, Mustermann John-3!

wir laden Sie herzlich dazu ein, sich mit dem Trainingsmodul "Passwörter und Konten: Anfänger" zu beschäftigen.

Wenn Sie das Thema der Einheit bereits kennen, können Sie einfach einen Test durchführen, um Ihr Wissen nachzuweisen. Andernfalls empfehlen wir, alle Lektionen der Einheit zu studieren und den abschließenden Test zu absolvieren.

[LERNEN BEGINNEN](#)

---

Motivation für das Training

Etwa 90 % aller Passwörter können gehackt werden. Viele

# ASAP – Benutzer-GUI

The screenshot displays the 'Kursverlauf' (Course Progress) page for a user named John-3. The interface is in German. At the top right, the user's name 'John-3' and the language 'Deutsch' are visible. A notification bell icon is present on the left. The main heading states 'Ihre aktuelle Trainingsstufe ist Anfänger' (Your current training level is Beginner). Below this, two training modules are listed: 'PASSWÖRTER UND KONTEN: ANFÄNGER' and 'E-MAIL: ANFÄNGER', each with a 'Starten' (Start) button. The first module includes an icon of a laptop with a padlock and text explaining password security. The second module includes an icon of an envelope and text explaining email security. On the right side, a dark sidebar shows a progress ring for 'Mein Ziel GRUNDLAGEN' (My Goal: Basics) with a green segment. Below the ring, it shows 'Geplantes Abschlussdatum' (Planned completion date) as 12.09.2019 and 'Voraussichtliches Abschlussdatum' (Estimated completion date) as 04.08.2019, with a 'Dem Plan voraus' (Ahead of schedule) button.

Kursverlauf

John-3 Deutsch

Willkommen zurück, John-3!  
Sie befinden sich in der aktiven Phase Ihres Trainings.

## Ihre aktuelle Trainingsstufe ist Anfänger

**PASSWÖRTER UND KONTEN: ANFÄNGER** Starten

 Etwa 90 % aller Passwörter können gehackt werden. Viele benutzen einfache Passwörter in dem Glauben, dass niemand versuchen würde, ihren Account zu hacken. Diese Menschen irren sich. Jeder Account kann gehackt werden, selbst wenn der Inhaber sich selbst nicht für verlockende Beute hält.

Hat er einmal das richtige Passwort, kann der Angreifer sich für Sie ausgeben und Bekannte und Freunde um Geld bitten, Malware über Ihre Kontaktliste verschicken, zweifelhafte Inhalte auf Ihrer Seite veröffentlichen oder Geld von Ihrem Bankkonto abheben. Darum ist es wichtig zu wissen, wie man mit wichtigen Passwörtern umgehen sollte.

**E-MAIL: ANFÄNGER** Starten

 Die E-Mail ist das wichtigste Kommunikationswerkzeug von Unternehmen. Fast jeder Internetnutzer hat einen E-Mail-Account. In der Regel werden diese Accounts verwendet, um sich für andere Dienstleistungen anzumelden. Wenn Ihr E-Mail-Account kompromittiert ist, erhält der Angreifer Zugang zu Ihrer Arbeitskorrespondenz oder zu ihren Bankdaten. E-Mails von Cyberkriminellen könnten Dateien und/oder Links enthalten, die Ihnen persönlich oder Ihrem Unternehmen Schaden zufügen können.

Mein Ziel  
**GRUNDLAGEN**

Geplantes Abschlussdatum  
📅 12.09.2019

Voraussichtliches Abschlussdatum  
📅 04.08.2019

[Dem Plan voraus](#)

Kaspersky

# ASAP – Benutzer-GUI

[Schließen](#) [Fehler/Tippfehler melden](#) John-3

## FRAGE 3

Was ist so gefährlich daran, jemand anderem mein Passwort zu einem sozialen Netzwerk weiterzugeben?

Wählen Sie die richtigen Antworten und drücken Sie ANTWORTEN

 <p>Betrüger könnten mein Profil übernehmen. <input checked="" type="checkbox"/></p>	 <p>Kriminelle könnten mein Bankkonto leerräumen. <input type="checkbox"/></p>	 <p>Betrüger könnten in meinem Namen online etwas kaufen, ich würde dabei Geld verlieren. <input type="checkbox"/></p>	 <p>Dieses eine Foto vom letzten Jungesellenabschied wird im gesamten Internet die Runde machen. <input type="checkbox"/></p>
 <p>Spam wird von meinem Account aus versendet werden. <input type="checkbox"/></p>	 <p>Ich verliere wichtige Informationen. <input type="checkbox"/></p>	 <p>Ich verliere alle Spielgegenstände und Ressourcen in meinem Online-Lieblingsspiel. <input type="checkbox"/></p>	 <p>Nichts Schlimmes wird passieren. <input type="checkbox"/></p>

[ZURÜCK](#) [ANTWORTEN](#)

# ASAP – Benutzer-GUI – Simulierte Phishing-Angriffe

## SIE SIND AUF EINE PHISHING-E-MAIL HEREINGEFALLEN!



Sie haben Glück. Diese E-Mail ist nur ein V  
Grundlage des abgeschlossenen Themas

Wäre dies ein echter Angriff, könnten die

- Zugang zu Ihren Konten erhalten
- Ihre persönlichen Daten stehlen
- Zugriff auf vertrauliche Informationen
- Malware auf Ihrem Computer installieren

In "E-Mail: Grundlagen" haben wir besprochen, warum es notwendig ist, alle in E-Mails erhaltenen Links sorgfältig zu analysieren. Bewegen Sie den Mauszeiger über den Link, bevor Sie ihn aufrufen, und stellen Sie sicher, dass der Text des Links der Site entspricht, zu der er angeblich führt.

Wenn Sie dies nicht tun, könnten Sie auf einer Website landen, die versuchen wird, Ihnen die Anmeldedaten für Ihre Unternehmensressourcen oder Bankkonten zu entlocken oder Malware installiert, die

- alle Dateien auf Ihrem Gerät sperrt und ein Lösegeld verlangt, um sie zu entschlüsseln.
- Ihre Anmeldedaten für wichtige Ressourcen stiehlt, einschließlich der Anmeldeinformationen für Ihre Unternehmens- und Bankkonten.
- ohne Ihr Wissen das Mikrofon und die Webcam einschalten kann, um Aufnahmen zu machen.

Welche Warnzeichen hätten Sie beachten sollen?

- Der angeblich von Dropbox stammende Link hat



## WAS SOLLTEN SIE TUN, WENN SIE EINE PHISHING-E-MAIL ERHALTEN?

- Drücken Sie keine aktiven Elemente in der E-Mail und speichern Sie keine Dateien aus dieser E-Mail
- Melden Sie den Erhalt der E-Mail den Mitarbeitern, die für die Sicherheit in Ihrem Unternehmen verantwortlich sind
- E-Mail löschen

Bitte drücken Sie diesen Button, um zu bestätigen, dass Sie die obigen Empfehlungen gelesen haben:

Bestätigen

kaspersky

# Kaspersky ASAP Phishing Simulator

# ASAP – Phishing Simulator

- Beliebige Benutzer können ausgewählt werden
- Vorhandene Templates/Vorlagen
- individuelle Anpassung der Phishing E-Mail mit Betreff, Texten und Bildern
- Auswahl der Phishing-Domain und Absender-E-Mail-Adresse aus einer Liste
- freie Planung der Kampagne
- Berichte pro Kampagne: Gesendete E-Mails, geöffnete E-Mails, Klickrate, Bestätigungen
- "Failure Tag" für Benutzer

# ASAP – Phishing Simulator

Dashboard Nutzer Trainingsgruppen Inhalt **Phishing-Simulator** Firmeneinstellungen

## PHISHING-SIMULATOR

Kampagnen E-Mail-Vorlagen

Anzahl der Kampagnen **2**

- Geplant 0
- Aktiv 2
- Abgeschlossen 0
- Abgebrochen 0

[Kampagne erstellen](#)

Name	Teilnehmer	Gesendete E-Mails	Geklickt	Gefährdungs...	Beginn des Versands	Ende des Versands	Enddatum der Datenerfass...	Status
<a href="#">Test-2_EN</a>	2	2	2	–	29.07.2020	29.07.2020	05.08.2020	Läuft

# ASAP – Phishing Simulator

Dashboard Nutzer Trainingsgruppen Inhalt **Phishing-Simulator** Firmeneinstellungen

## PHISHING-SIMULATOR

Kampagnen **E-Mail-Vorlagen**

Deutsch ▼ Gefährdungsgrad ▼ System Benutzerdefiniert

Name	Betreff	Name des Absenders	Adresse	Gefährdungsgr...	Kategorie	Verfügbare Sprachen			
Neues Kalenderereignis	Neues Kalenderereignis	Ecalendar	service@ecalend..	33%	Allgemein, Kalender & Veranstaltungen	AR, DE, EN, ES, FR, IT, RU	✉	👁	⋮
BestTaste: Unternehmensra... in Restaurants	Unternehmensra... auf Top-Marken	BEST TASTE	best-taste@business-information.store	50%	Geschäftlich, Unternehmensdi... Werbung	AR, DE, EN, ES, FR, IT, RU	✉	👁	⋮
UPS: Zustellversuch fehlgeschlagen	Zustellversuch fehlgeschlagen	Postversand	service@thedeliv..	29%	Allgemein, E-Mail und Lieferung	AR, DE, EN, ES, FR, IT, RU	✉	👁	⋮

kaspersky

# **Benutzer-Synchronisation mit MS Azure AD & SSO – NEU –**

# ASAP – User-Sync mit MS Azure AD & ADFS

The screenshot displays the ASAP user management interface. At the top, a navigation bar includes 'Dashboard', 'Nutzer', 'Trainingsgruppen', 'Inhalt', 'Phishing-Simulator', 'Neu', and 'Firmeneinstellungen'. Below this, the 'NUTZER' section is visible. A secondary navigation bar within the content area includes 'Dashboard', 'Nutzer', 'Trainingsgruppen', 'Inhalt', and 'Phishing-Simulator'. The main content area is titled 'IMPORT UND SYNCHRONISIERUNG' and features two tabs: 'Import' and 'SCIM'. The 'SCIM' tab is active. The text under the 'SCIM' tab explains that user data from Active Directory can be synchronized automatically using the SCIM protocol. It notes that users will be automatically added, changed, and archived once SCIM is configured, and that the synchronization is one-way. A 'Testmodus' toggle is currently turned on. At the bottom, the 'Mandanten-URL' is listed as 'https://asap-api.k-asap.eu/scim/v2' with a copy icon. On the right side of the interface, there are two buttons: 'Archivierte Nutzer zeigen' and 'Import und Synchronisierung'. The 'Import und Synchronisierung' button is circled in red. Below it is another button labeled 'Nutzer hinzufügen'.

# ASAP – SSO (Single Sign-On)

Dashboard Nutzer Trainingsgruppen Inhalt Phishing-Simulator Neu Firmeneinstellungen

## FIRMENEINSTELLUNGEN

Allgemein Benutzerdefinierte Felder und Regeln Einstellungen für die Anrede **SSO**

Sie können den Benutzerzugriff auf die ASAP-Plattform mithilfe der Single Sign-On-Technologie (SSO) konfigurieren. Die SSO-Authentifizierung ist standardmäßig deaktiviert. Benutzer können über persönliche Links in ihren Schulungseinladungen auf die Lernplattform zugreifen.

Sobald SSO aktiviert ist, können die Benutzer mit den Anmeldedaten eines Identitätsanbieters auf die Lernplattform zugreifen. Eine ausführliche Anleitung finden Sie [hier](#).

SAML deaktiviert ?

URL des Identitätsanbieters\*

Entitäts-ID\*

Signaturzertifikat\*  
(PEM im X.509-Format)

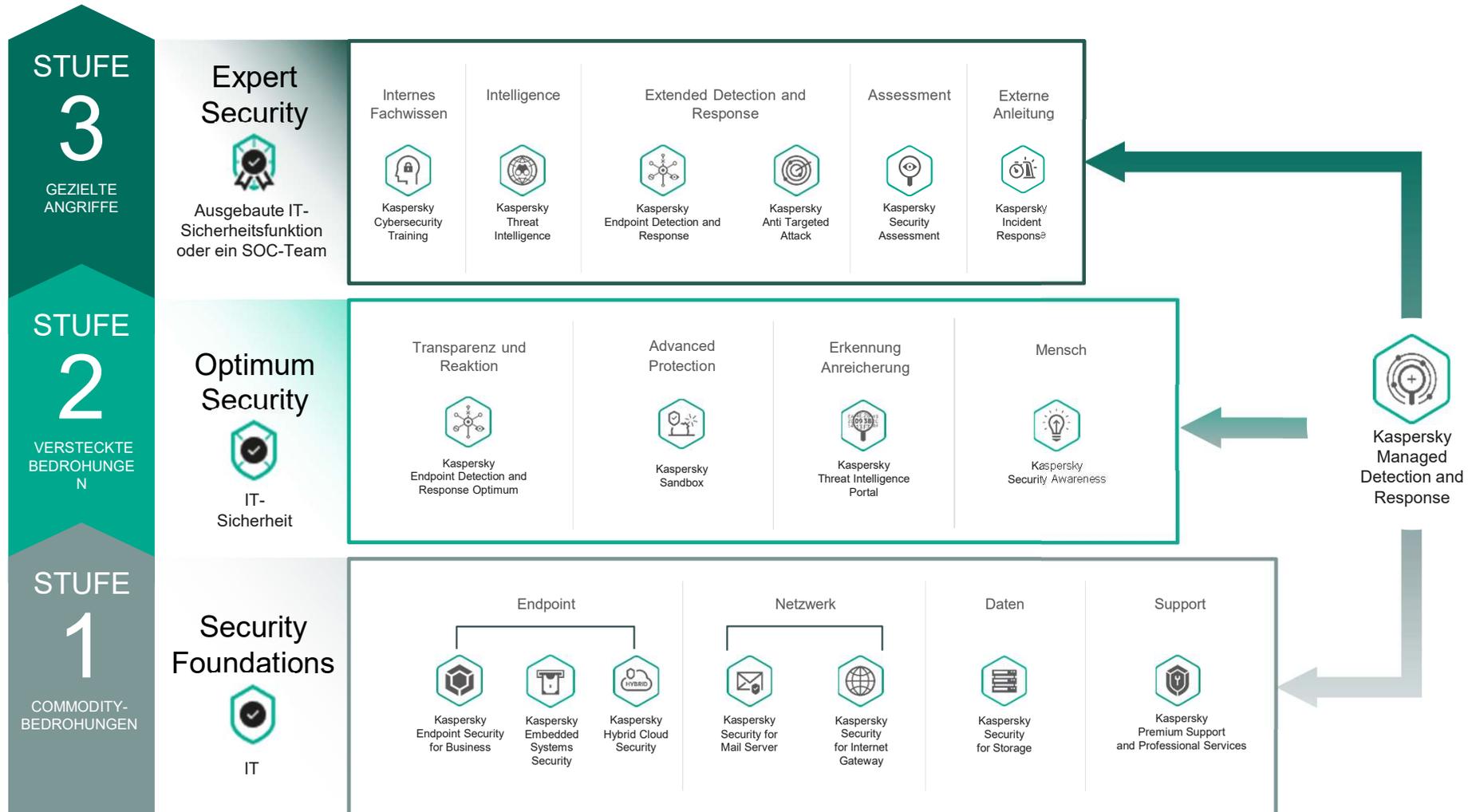
# ASAP – Was benötigen Sie, um zu beginnen ?

1. ASAP – Landing-Page (Trial/Test für 5 User und 2 Monate)  
<https://www.k-asap.com/> (https://app.k-asap.eu/)
2. Registrierung für den Admin-Account – anschl. Einladungs-Email von Kaspersky
3. Mit ASAP starten...



manuell bei z.B. Trial oder  
automatisiert via vorher  
definierten Gruppenregeln

# Kasperskys Cybersicherheitskonzept – Schritt für Schritt



kaspersky

Vielen Dank

Stefan Zysset / *Senior Presales Engineer* / [stefan.zysset@kaspersky.com](mailto:stefan.zysset@kaspersky.com)

Michael Zeger / *Territory Manager Austria* / [michael.zeger@kaspersky.com](mailto:michael.zeger@kaspersky.com)

[kaspersky.com](https://kaspersky.com)