Sicherheit

- E-Mail-Sicherheit / HornetSecurity / E-Mail-Archivierung
- E-Mail-Sicherheit / HornetSecurity / Benutzerlogin und Verwaltung
- Internet-Sicherheit - DNS - Welche DNS-Server bieten welchen Schutz?
- Installation unserer ACP-Agents aus dem MSP-Paket
- E-Mail-Sicherheit / HornetSecurity / Security Awareness Service / Ablauf und Reaktionen
- E-Mail-Sicherheit / HornetSecurity / Security Awareness Service / UserPanel

E-Mail-Sicherheit / HornetSecurity / E-Mail-Archivierung

Kurzbeschreibung: Die in HornetSecurity enthaltene E-Mail-Archivierung (lizenzabhängig) bedarf keiner umfangreichen Konfiguration und Anpassung. Sie funktioniert „out-of-the-box" und stellt die revisionssichere Archivierung sicher. Dieser Artikel zeigt, wie man sich im UserPanel einloggt und die Archivierung anpasst oder archivierte Mails findet.

Für wen relevant?

- Alle Nutzer, deren Postfach über HornetSecurity revisionssicher archiviert wird und die archivierte E-Mails suchen oder einzelne E-Mails als „privat" markieren möchten.

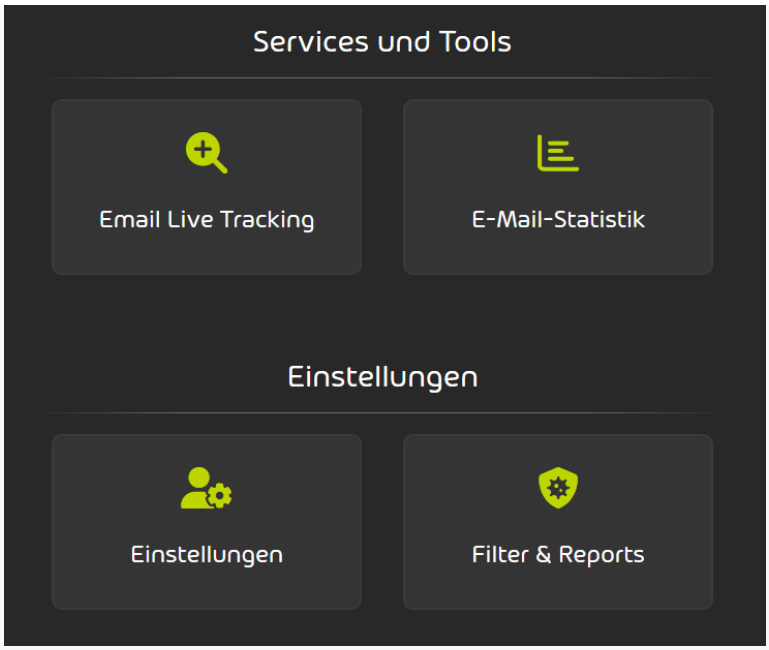
Kurze Erklärung – Was ist bei der Archivierung wichtig?

- Aus rechtlichen Gründen kann es notwendig sein, bestimmte E-Mails von der Sichtbarkeit durch Dritte (z. B. Revisoren/Auditoren) in der Archivierung auszunehmen. Dies erfolgt in HornetSecurity einfach über die nachträgliche Markierung als **„privat"**.
- Die Aufbewahrungszeit für die E-Mail-Archivierung beträgt im Standard voreingestellt **10 Jahre**. E-Mails, die älter als 10 Jahre sind, werden automatisch vom System gelöscht – ein manueller Eingriff ist nicht nötig.

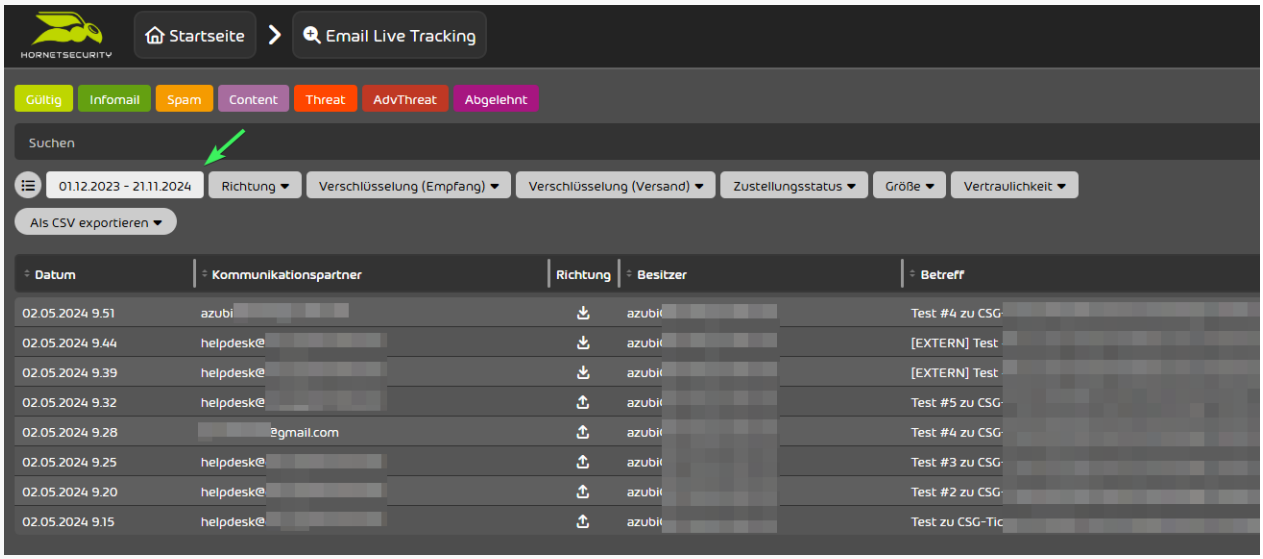
Hinweis Eine offizielle und umfangreiche Anleitung findet sich in der Anleitung zum UserPanel von HornetSecurity sowie in der detaillierten Anleitung zur Nutzung des Archivs in der KnowledgeBase von HornetSecurity.

Schritt-für-Schritt-Anleitung

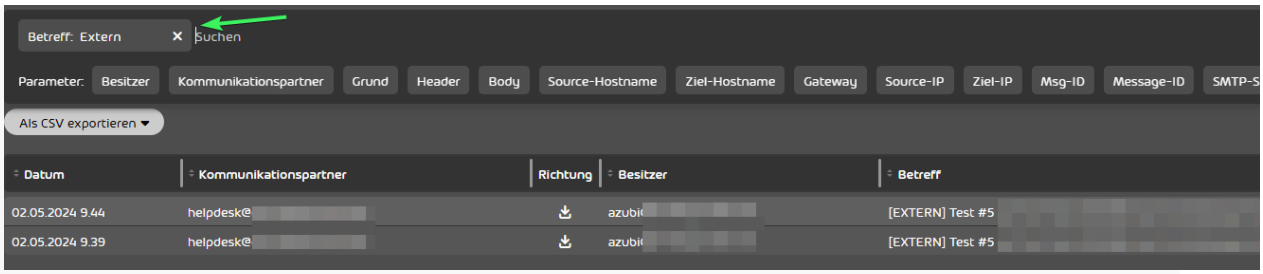
1. Login zum UserPanel für Benutzer unter https://cp.hornetsecurity.com/user_dashboard. Die Anmeldung erfolgt über die E-Mail-Adresse, das Passwort und die Multi-Faktor-Authentifizierung von Microsoft 365.
2. Das UserPanel wird geöffnet.



3. **E-Mail-Livetracking** wird geöffnet und zeigt alle E-Mails, abhängig vom ausgewählten Zeitfenster rechts oben.

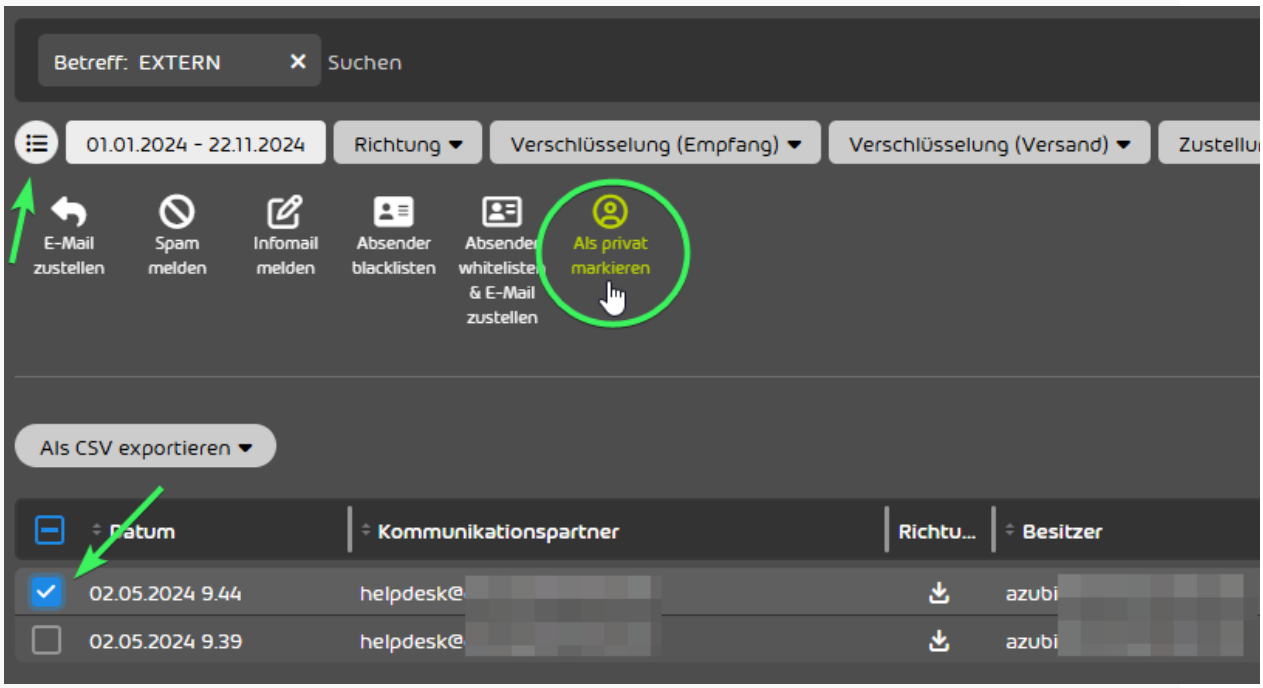


4. Über die Suchfunktion kann eine gewünschte E-Mail gesucht werden, wobei eine Vielzahl von Auswahlfiltern zur Verfügung steht (im Beispiel: Suche nach „Extern" im „Betreff").



Hinweis Der Suchtext muss immer mindestens 3 Zeichen enthalten.

5. Benutzer dürfen E-Mails als „privat" markieren, damit diese nicht durch Auditoren/Revisoren eingesehen werden können – dies ist z. B. bei Bewerbungsschreiben relevant. Dazu klickt man links oben auf das E-Mail-Menü, wählt die entsprechende E-Mail aus und klickt auf **„Als privat markieren"**.



Achtung Um diese Funktion nutzen zu können, ist es notwendig, dass der Administrator die Funktion zuvor freigeschaltet hat.

Kurze Checkliste

- Login im UserPanel über https://cp.hornetsecurity.com/user_dashboard mit M365-Zugangsdaten und MFA erfolgreich?
- Gewünschte E-Mail über das E-Mail-Livetracking bzw. die Suchfunktion (mind. 3 Zeichen) gefunden?
- Bei Bedarf: E-Mail über das E-Mail-Menü als „privat" markiert?
- Freischaltung der „Privat"-Funktion durch den Administrator sichergestellt, falls diese fehlt?

FAQ – kurz & knapp

- Wie lange werden meine E-Mails archiviert?
  - Im Standard 10 Jahre; ältere E-Mails werden automatisch und ohne manuellen Eingriff gelöscht.
- Wer kann archivierte E-Mails einsehen?
  - Grundsätzlich können Auditoren/Revisoren auf archivierte E-Mails zugreifen, sofern diese nicht als „privat" markiert wurden.
- Warum finde ich die Funktion „Als privat markieren" nicht?
  - Diese Funktion muss zunächst vom Administrator freigeschaltet werden.
- Wie melde ich mich im UserPanel an?
  - Über https://cp.hornetsecurity.com/user_dashboard mit der E-Mail-Adresse, dem Passwort und der Multi-Faktor-Authentifizierung Ihres Microsoft-365-Kontos.

Fußzeile
Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: faq-hornetsecurity-archivierung

E-Mail-Sicherheit / HornetSecurity / Benutzerlogin und Verwaltung

Kurzbeschreibung: Dieser Artikel zeigt, wie Sie sich als Benutzer bei HornetSecurity anmelden und welche Hauptfunktionen (E-Mail Live Tracking, Filter & Reports, Black- & Whitelists) Ihnen nach dem Login zur Verfügung stehen.

Für wen relevant?

- Alle Benutzer, deren Postfach über HornetSecurity abgesichert wird und die sich im HornetSecurity-Portal anmelden und dort verwalten möchten (z. B. Quarantäne, Absenderlisten).

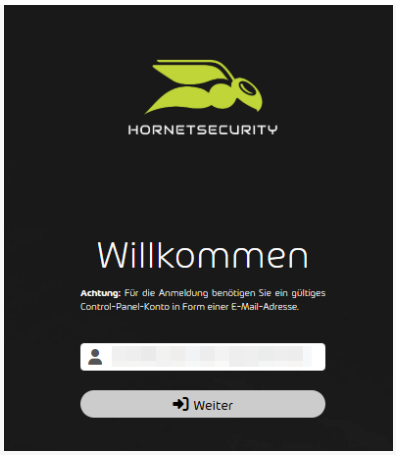
1. Anmeldung bei HornetSecurity

Um sich als Benutzer bei HornetSecurity anzumelden, besuchen Sie folgende Webseite:

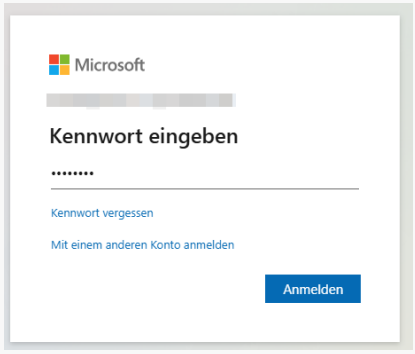
HornetSecurity Login

Schritte zur Anmeldung:

1. Geben Sie Ihre E-Mail-Adresse als Benutzernamen ein.



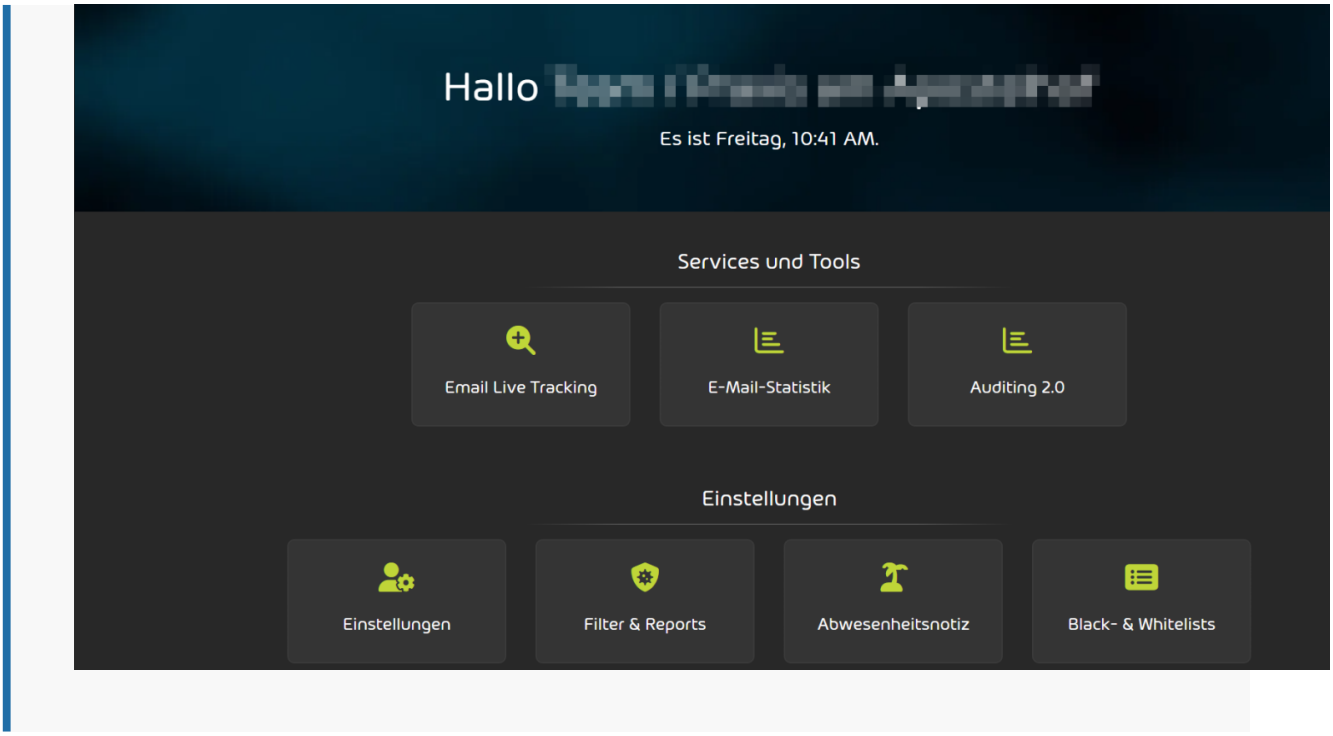
2. Sie werden zur Microsoft-Anmeldeseite weitergeleitet.



3. Geben Sie das zugehörige Passwort ein.
4. Nach erfolgreicher Authentifizierung gelangen Sie auf die Startseite von HornetSecurity.

2. Navigation in der Weboberfläche

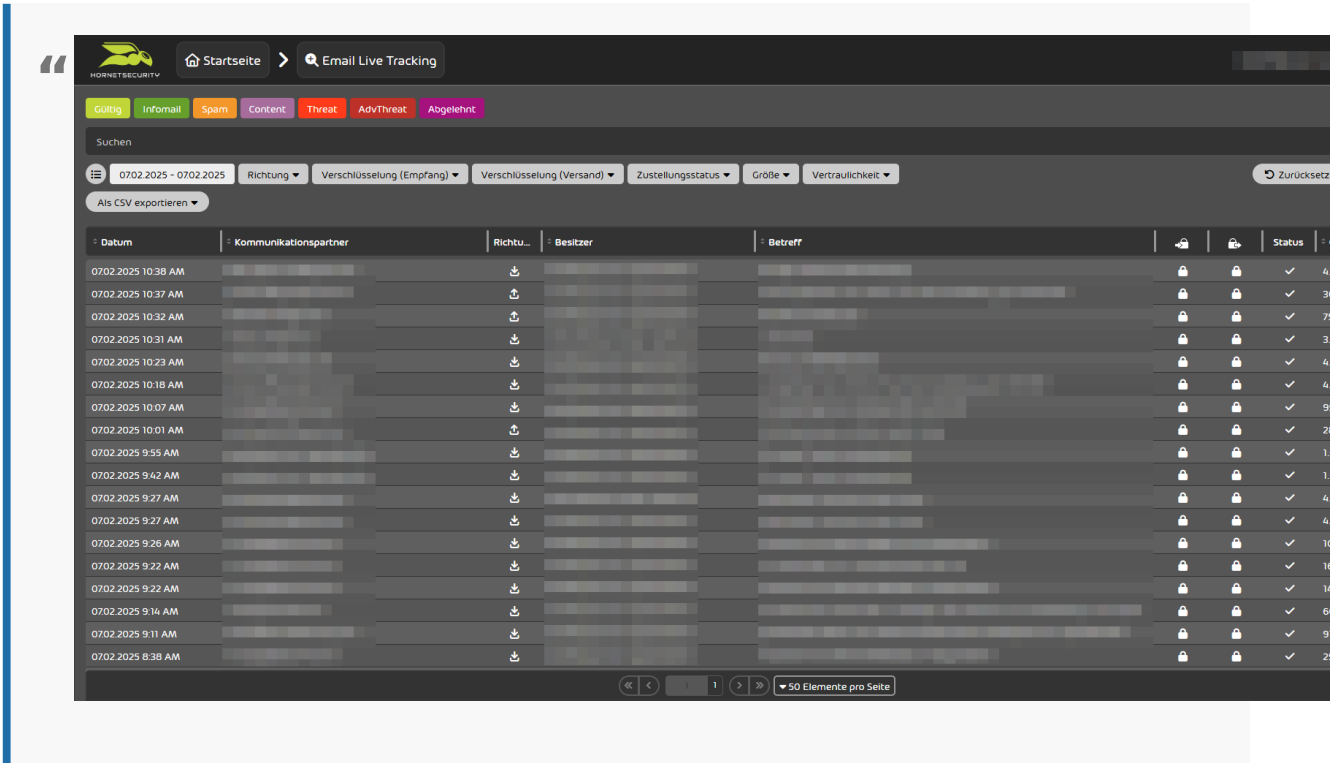
Nach dem Login stehen Ihnen folgende Hauptfunktionen zur Verfügung:



- **E-Mail Live Tracking** – Überwachung des ein- und ausgehenden E-Mail-Verkehrs.
- **Filter & Reports** – Verwaltung von Quarantäne-Berichten und Sicherheitsfiltern.
- **Black- & Whitelists** – Verwaltung der zugelassenen und blockierten Absender.

2.1 E-Mail Live Tracking

Im E-Mail Live Tracking können Sie den Verlauf eingehender und ausgehender E-Mails überprüfen.



- **Suchleiste**: Ermöglicht die gezielte Suche nach Mails anhand des Absendernamens oder eines Begriffs aus dem Betreff.

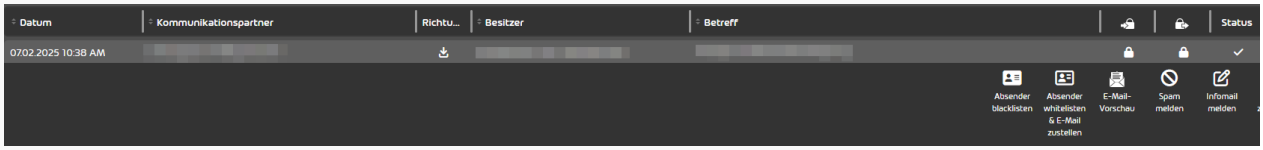
- **Symbole:**
  - Eingehende E-Mails

    > 

  - Ausgehende E-Mails

    > 

- **Aktionen:**

  > 
  >

- **Mails aus Quarantäne zustellen:** Durch Klick auf den Pfeil rechts wird die E-Mail ausgeklappt und kann bearbeitet werden.
- **Absender blockieren (Blacklist):** Blockiert den Absender, sodass dieser keine E-Mails mehr senden kann.
- **Absender freigeben & Mail zustellen (Whitelist):** E-Mails dieses Absenders werden zukünftig nicht mehr als Spam markiert.
- **E-Mail-Vorschau:** Zeigt den Inhalt der E-Mail in einem separaten Fenster an.
- **Spam melden:** Markiert die E-Mail als Spam.
- **Infomail melden:** Kennzeichnet die E-Mail als Newsletter oder Werbemail.
- **Als privat markieren:** Markiert die E-Mail als vertraulich (wichtig für die Archivierung).
- **Technische Informationen anzeigen:** Zeigt wichtige Details für Administratoren.

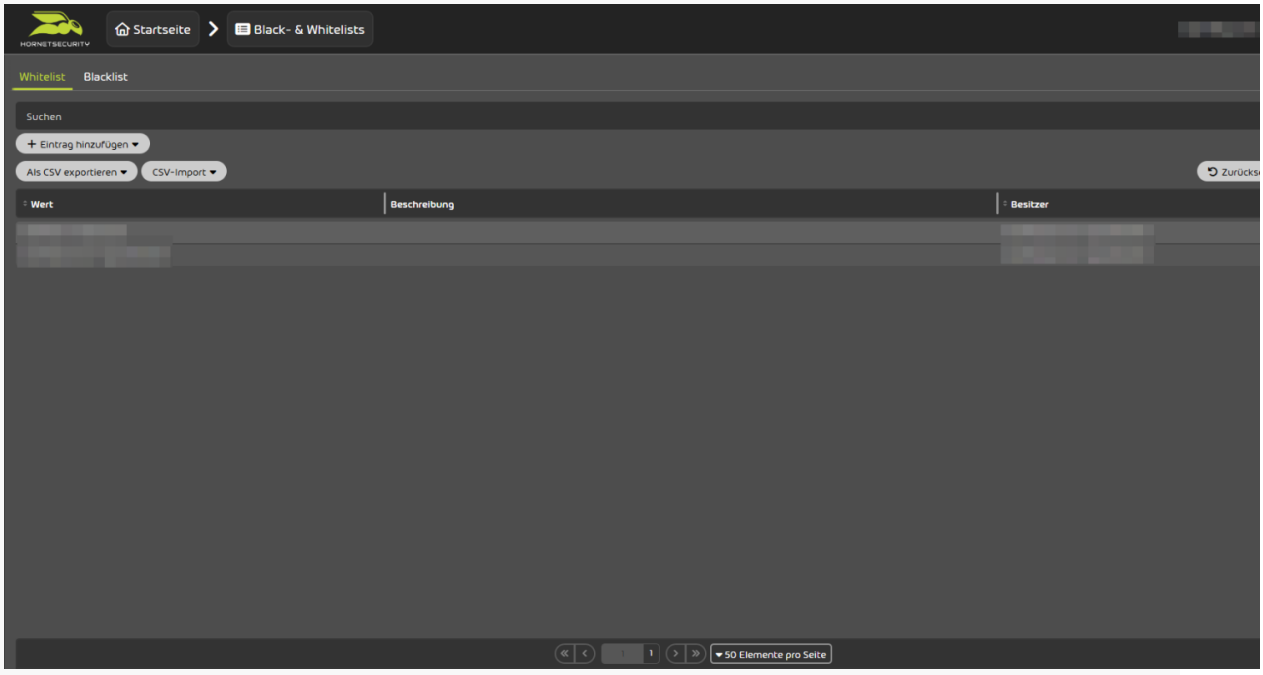
Achtung Von der Nutzung von **„Absender freigeben & Mail zustellen (Whitelist)"** raten wir ausdrücklich ab, da dies die Sicherheit der E-Mails massiv reduziert.

2.2 Filter & Reports

Hier können Benutzer individuelle Einstellungen für Quarantäne-Berichte und Filteroptionen vornehmen.

2.3 Black- & Whitelist

Diese Sektion bietet eine Übersicht über blockierte (Blacklist) und freigegebene (Whitelist) Absender. Neue Einträge können manuell hinzugefügt oder bestehende Einträge bearbeitet werden.



Achtung Auch hier gilt: Wir empfehlen die Nutzung des Whitelistings **nicht**, da es die Sicherheit von E-Mails massiv reduziert.

Kurze Checkliste

- Anmeldung über https://cp.hornetsecurity.com/ mit E-Mail-Adresse und anschließender Microsoft-Authentifizierung erfolgreich?
- Gewünschte E-Mails über das E-Mail Live Tracking gefunden und ggf. bearbeitet?
- Quarantäne-Berichte und Filteroptionen unter „Filter & Reports" bei Bedarf angepasst?
- Blacklist-Einträge zur Blockierung unerwünschter Absender genutzt (statt Whitelisting)?

FAQ – kurz & knapp

- Mit welchen Zugangsdaten melde ich mich bei HornetSecurity an?
  - Mit Ihrer E-Mail-Adresse als Benutzername; die eigentliche Authentifizierung erfolgt anschließend über Ihr Microsoft-365-Konto.
- Warum sollte ich Absender nicht auf die Whitelist setzen?
  - Weil dadurch E-Mails dieses Absenders zukünftig nicht mehr auf Spam/Schadinhalt geprüft werden – das reduziert die E-Mail-Sicherheit massiv. Blockieren (Blacklist) einzelner Absender ist hiervon nicht betroffen und unbedenklich.
- Was bedeutet „Als privat markieren" im Live Tracking?
  - Die E-Mail wird als vertraulich gekennzeichnet, was insbesondere für die revisionssichere Archivierung relevant ist.
- Wo finde ich Quarantäne-Berichte und Filtereinstellungen?
  - Unter dem Menüpunkt „Filter & Reports" im HornetSecurity-Portal.

Fußzeile Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: https://csg.gmbh/faq-hornetsecurity-login-verwaltung

Internet-Sicherheit - DNS - Welche DNS-Server bieten welchen Schutz?

Kurzbeschreibung: Sicherheit in der IT, speziell auch bei der Verbindung ins Internet, ist ein vielschichtiges Thema. Es gibt keine Einzellösung mit maximalem Schutz, sondern nur sich ergänzende Module wie z. B. E-Mail-Sicherheit, Virenscanner, Firewall, Patchmanagement und vieles mehr. Ein kleiner, aber wichtiger und effektiver Baustein ist die Absicherung des DNS (Domain Name System) – konkret die Wahl eines sicheren DNS-Servers.

Für wen relevant?

- Alle, die ihre Internetverbindung durch die Wahl eines sicherheitsfokussierten DNS-Servers zusätzlich absichern möchten.

Kurze Erklärung – Warum ist der DNS-Server wichtig?

- Auf das Wichtigste heruntergebrochen stellt die Auswahl eines sicheren DNS-Servers das Herz der DNS-Absicherung dar.
- Von den DNS-Servern der Provider ist hier nicht generell abzuraten, jedoch stellen speziell auf Absicherung von Internetanfragen ausgelegte DNS-Server oftmals die zielführendere Wahl dar.

Hinweis Folgende DNS-Server werden hier genannt, ohne Anspruch auf Vollständigkeit und dauerhafte Aktualität.

Übersicht sicherheitsfokussierter DNS-Server

Anbieter	IP-Adresse 1	IP-Adresse 2	Sicherheit
OpenDNS (Cisco)	208.67.222.222	208.67.220.220	Ohne spezielles Konto bieten diese DNS-Server das Blocken von bekannten Phishing-Seiten.

Anbieter	IP-Adresse 1	IP-Adresse 2	Sicherheit
VeriSign	64.6.64.6	64.6.65.6	Der Anbieter kommuniziert eine „allgemein höhere Sicherheit" durch Einsatz seiner DNS-Server, mit Fokus auf Stabilität und Privatsphäre.
Quad9	9.9.9.9	149.112.112.112	Hinter diesem Anbieter (organisiert als gemeinnützige Schweizer Stiftung) stehen verschiedene Hersteller und Organisationen, u. a. IBM, PCH, GCA, welche sich für mehr IT-Sicherheit einsetzen. Durch den Einsatz unterschiedlicher Blacklisten wird der Zugriff auf das Internet gegen Schadsoftware, Phishing und Missbrauch besser abgesichert.
Cloudflare (Sicherheitsvariante)	1.1.1.2	1.0.0.2	Blockiert bekannte Schadsoftware- und Phishing-Domains.
AdGuard DNS (Standard/Familie)	94.140.14.14	94.140.15.15	Blockiert Schadsoftware, Phishing und Tracking; eine Variante mit zusätzlicher Werbeblockierung ist ebenfalls verfügbar.
NextDNS	individuell je Konto	individuell je Konto	Konfigurierbarer Cloud-DNS-Dienst mit Schadsoftware-/Phishing-Blocking, Blocklisten und detaillierten Auswertungen; erfordert ein kostenloses Konto zur individuellen Konfiguration.

Achtung Die reine Standardadresse von Cloudflare (`1.1.1.1` / `1.0.0.1`) bietet **keinen** Schutz vor Schadsoftware – sie ist auf schnelle, private DNS-Auflösung ausgelegt, ohne Filterung. Erst die Sicherheitsvariante `1.1.1.2` / `1.0.0.2` blockiert bekannte Schadsoftware- und Phishing-Domains (eine zusätzliche Variante `1.1.1.3` / `1.0.0.3` blockiert zusätzlich Erwachseneninhalte).

Tipp Viele der genannten Anbieter unterstützen inzwischen verschlüsselte DNS-Abfragen über DNS-over-HTTPS (DoH) oder DNS-over-TLS (DoT). Das verhindert, dass DNS-Anfragen auf dem Übertragungsweg unverschlüsselt mitgelesen werden können – ein sinnvoller zusätzlicher Baustein, sofern Router bzw. Endgeräte dies unterstützen.

Unsere eigene Lösung: Securepoint Cloud Shield (by CSG)

Als zertifizierter Securepoint-Partner bieten wir Ihnen **Securepoint Cloud Shield** an – eine DNS-gestützte Sicherheitslösung, die Ihr gesamtes Netzwerk sowie internetfähige Geräte (auch Smart-TVs oder Netzwerkdrucker) auf DNS-Ebene absichert.

- **Funktionsweise:** Der gesamte DNS-Datenverkehr wird über sichere Securepoint-Server geleitet, wo gefährliche Verbindungen gestoppt werden, bevor sie zustande kommen. Jede Adresse wird vor dem Besuch mit einer stetig aktualisierten Sicherheitsdatenbank abgeglichen; bei einer sicheren Adresse baut Cloud Shield eine verschlüsselte Verbindung auf.
- **Kompatibilität:** Passt zu jeder Infrastruktur – kompatibel mit jedem Router, jeder Firewall und jedem VPN-Protokoll.
- **Wartungsaufwand:** 100 % Cloud-Service, komplett wartungsfrei, keine zusätzliche Hardware nötig.
- **Weitere Funktionen:** individuelle Content-Filter (z. B. für Jugendschutz), Geo-IP-Blocking (Sperrung von Verbindungen in bestimmte Länder), sowie Verwaltung und Auswertungen über ein Online-Portal.
- **Herkunft:** Securepoint ist ein deutscher Hersteller (Lüneburg) mit deutschem Rechenzentrum.

Unser Vertrieb berät Sie gern und informiert auch darüber, wie sich Cloud Shield in unser Gesamtangebot einfügt.

Weiterführende Informationen direkt bei Securepoint: Cloud Shield – Secure DNS

Kurze Checkliste

- Aktuell genutzten DNS-Server geprüft (Provider-Standard oder bereits ein sicherheitsfokussierter Anbieter)?
- Bei Cloudflare: sichergestellt, dass die Sicherheitsvariante (1.1.1.2/1.0.0.2) statt der Standardadresse genutzt wird, falls Schadsoftware-Blocking gewünscht ist?
- Verschlüsselte DNS-Abfragen (DoH/DoT) in Betracht gezogen, sofern Router/Endgeräte dies unterstützen?
- Individuelle Beratung zu Securepoint Cloud Shield gewünscht?

FAQ – kurz & knapp

- Reicht die Wahl eines sicheren DNS-Servers allein als Schutz aus?
  - Nein, DNS-Sicherheit ist nur ein Baustein von vielen (neben z. B. E-Mail-Sicherheit, Virenscanner, Firewall, Patchmanagement) und ersetzt keine der anderen Schutzmaßnahmen.
- Blockiert Cloudflares Standard-DNS (1.1.1.1) automatisch Schadsoftware?
  - Nein. Dafür ist die separate Sicherheitsvariante 1.1.1.2 / 1.0.0.2 nötig.
- Was ist der Unterschied zwischen den genannten kostenlosen Anbietern und Securepoint Cloud Shield?
  - Die kostenlosen Anbieter bieten meist eine feste, nicht individuell anpassbare Filterung. Securepoint Cloud Shield ist dagegen individuell konfigurierbar (Content-

Filter, Geo-IP-Blocking), wird über ein Online-Portal verwaltet und läuft auf deutscher Infrastruktur.

Fußzeile
Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: https://csg.gmbh/faq-dns-sicherheit

Installation unserer ACP-Agents aus dem MSP-Paket

Kurzbeschreibung: Es kann vorkommen, dass unser CSG-Team Sie bittet, vorbereitend die Kernkomponente (Agent) unseres MSP-Pakets zu installieren. Diese Anleitung führt Schritt für Schritt durch die Installation des Acronis Cyber Protect Agents.

Für wen relevant?

- Kunden, die vom CSG-Team gebeten wurden, den MSP-Agent auf bestimmten Rechnern vorbereitend zu installieren.

Was Sie vom CSG-Team erhalten

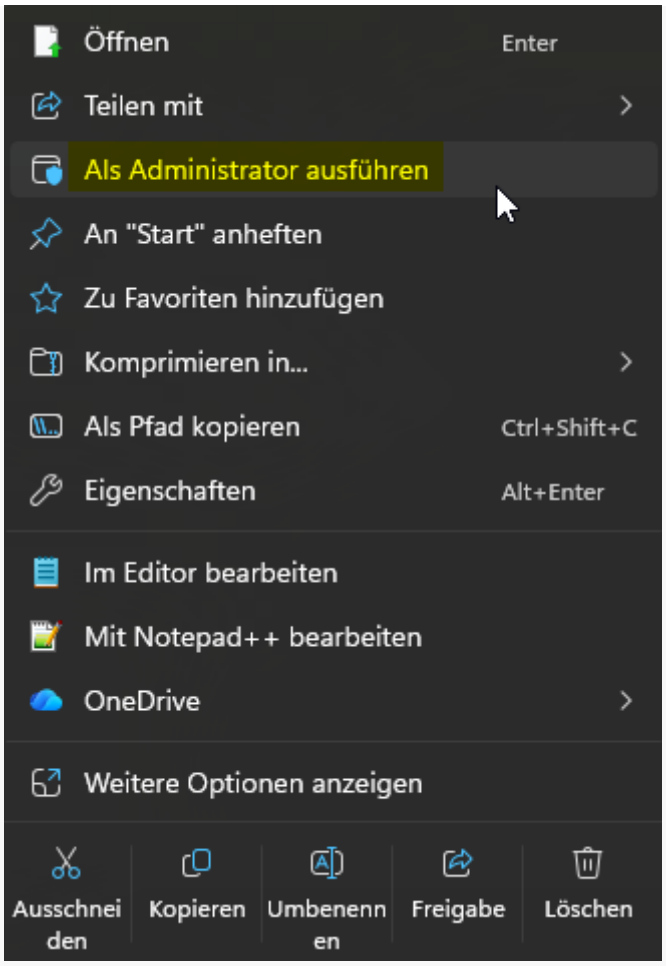
1. Einen Downloadlink für den MSP-Agent von Acronis.
2. Einen Token für die Registrierung des Agents.

Hinweis Das übermittelte Token hat im Regelfall eine Gültigkeitsdauer von einem Tag – bitte die Installation entsprechend zeitnah durchführen.

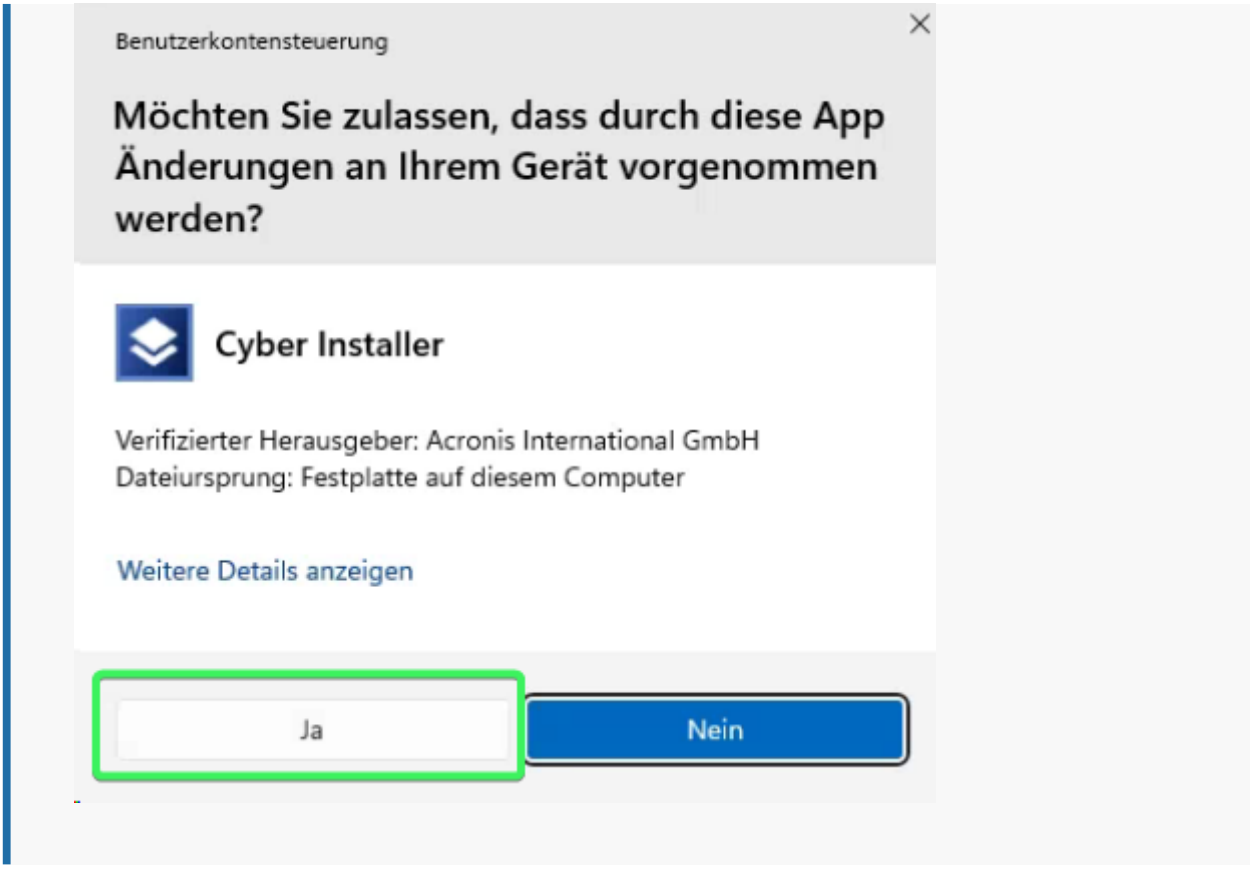
Schritt-für-Schritt-Anleitung

Bitte gehen Sie wie folgt an den eingeplanten Rechnern vor:

1. Melden Sie sich am Rechner mit Administratorrechten an.
2. Laden Sie die Datei über den Downloadlink herunter (typischer Dateiname: `CyberProtect_AgentForWindows_web.exe`).
3. Starten Sie die Datei mit der rechten Maustaste und der Auswahl **„Als Administrator ausführen"**.

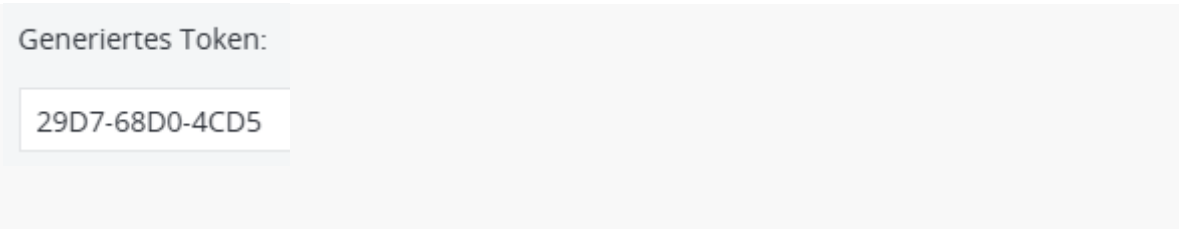


4. Bestätigen Sie die Meldung der Benutzerkontensteuerung mit **„Ja"**.

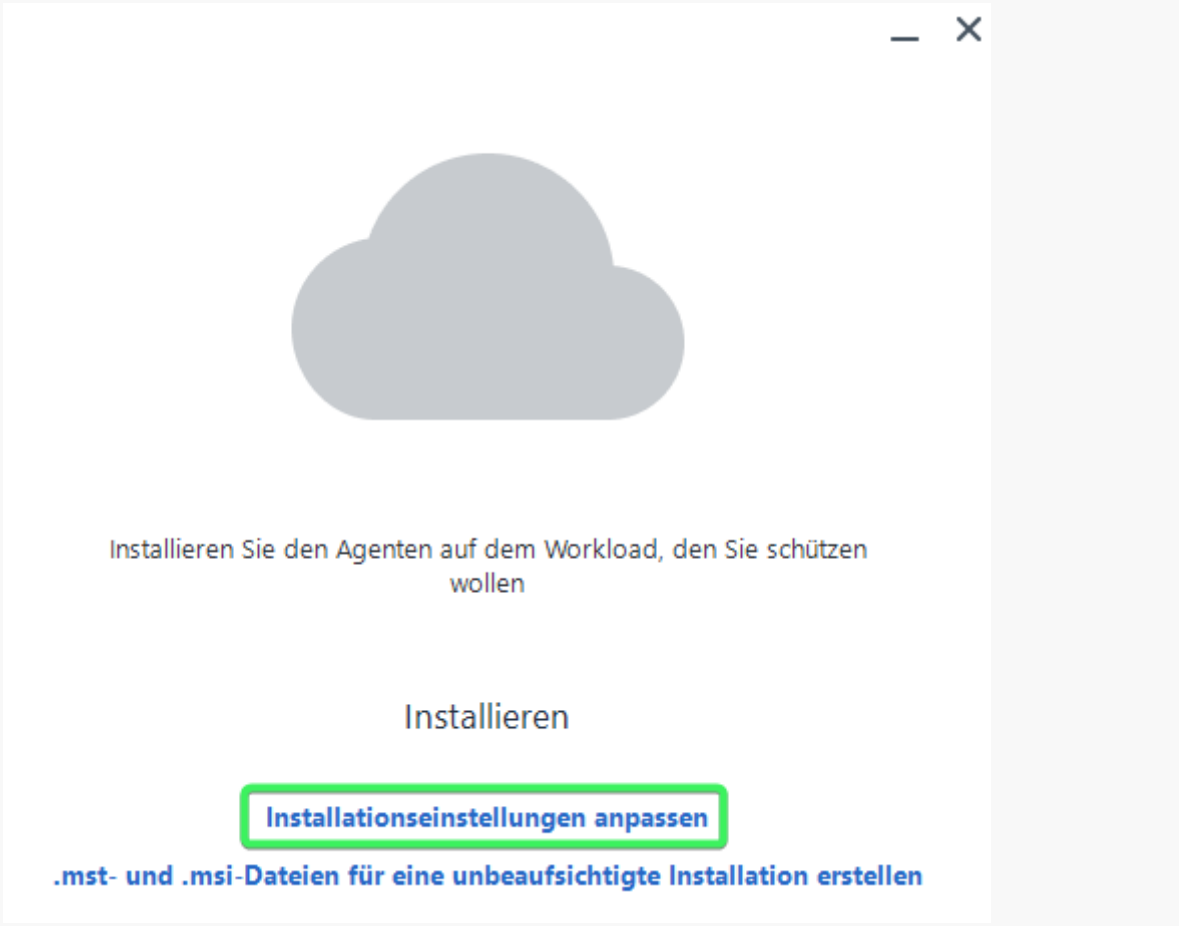


5. Es folgt eine Startmeldung des Installationsassistenten.

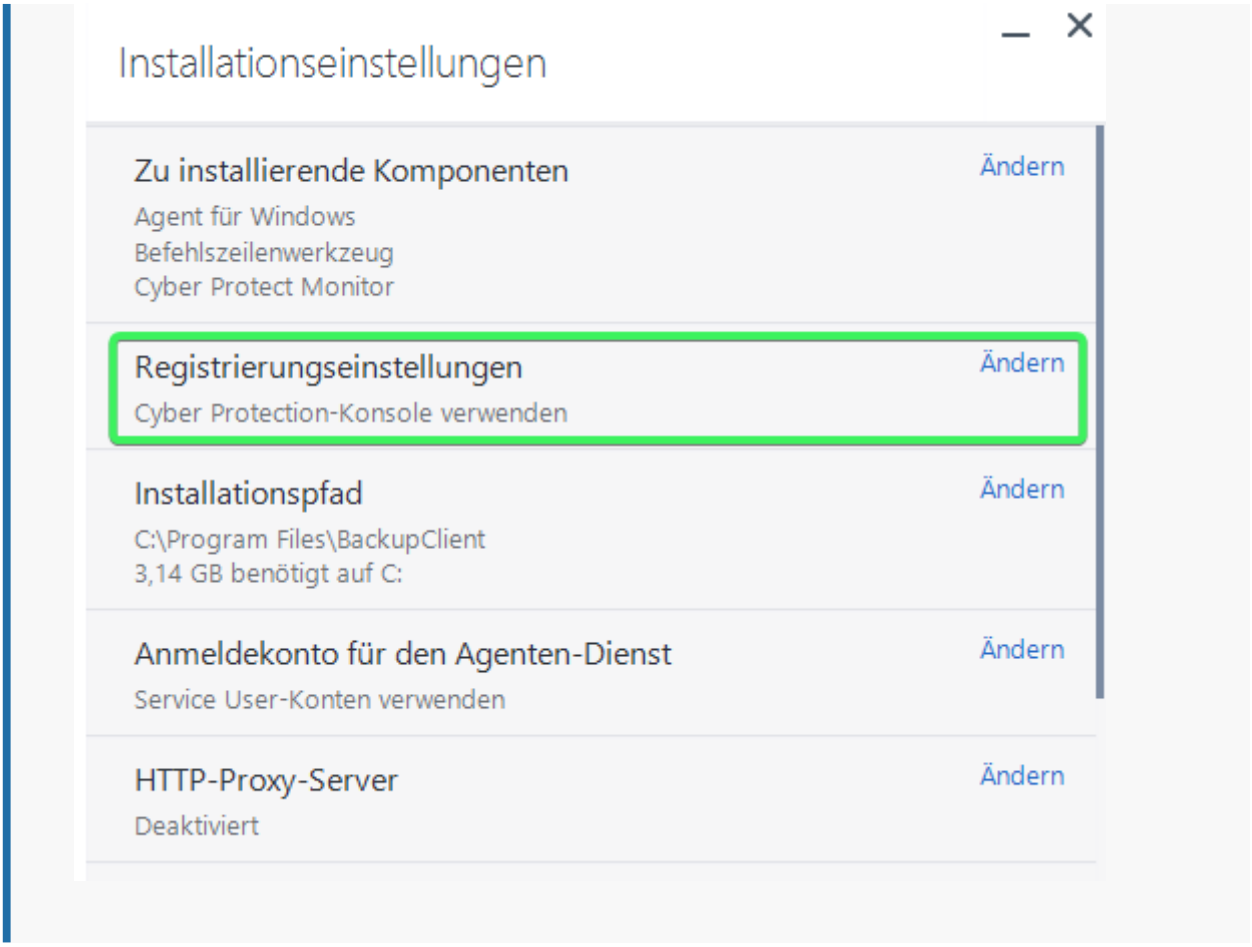
6. Halten Sie das übermittelte Token bereit.



7. Klicken Sie auf **„Installationseinstellungen anpassen"**.

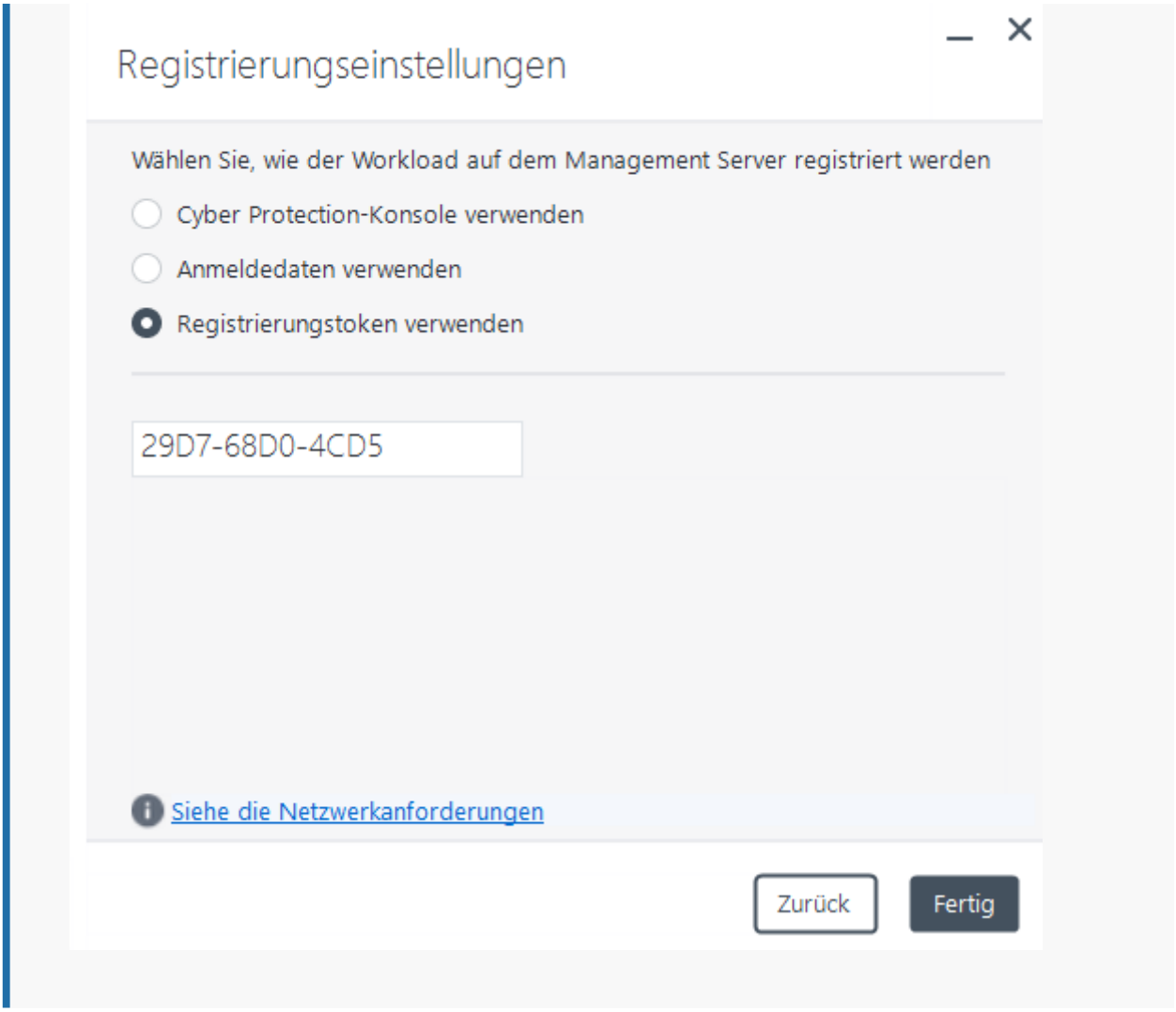


8. Wählen Sie in der folgenden Ansicht **ausschließlich** „Registrierungseinstellungen" → „ändern".

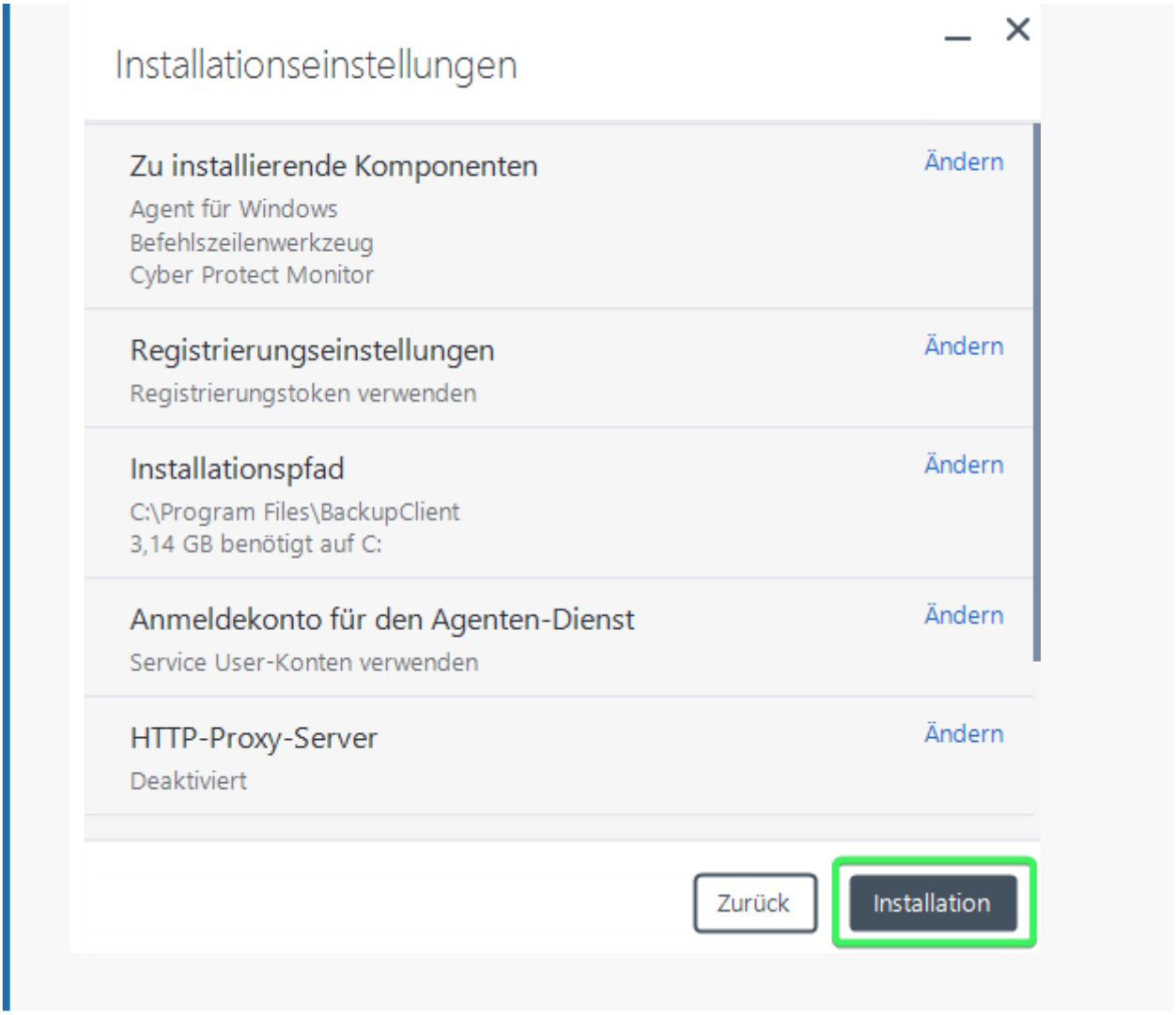


Achtung Passen Sie an dieser Stelle **keinesfalls** andere Einstellungen an – ändern Sie ausschließlich die Registrierungseinstellungen.

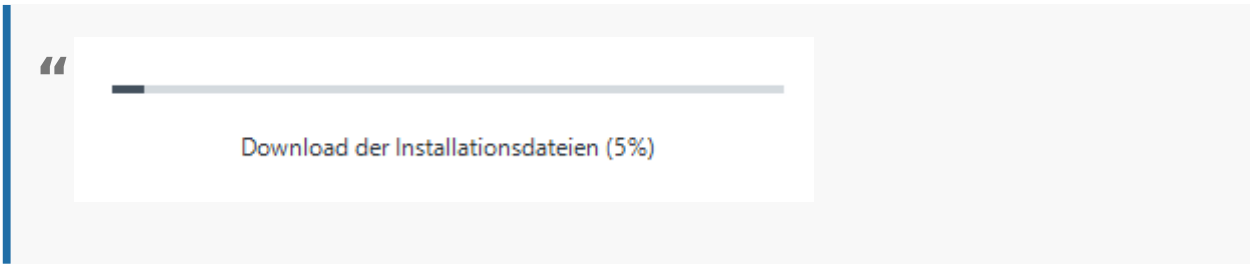
9. Wählen Sie **„Registrierungstoken verwenden"**, kopieren Sie das Token (siehe Schritt 6) in das Eingabefeld und klicken Sie auf **„Fertig"**.



10. Klicken Sie im nächsten Fenster auf **„Installation"**.

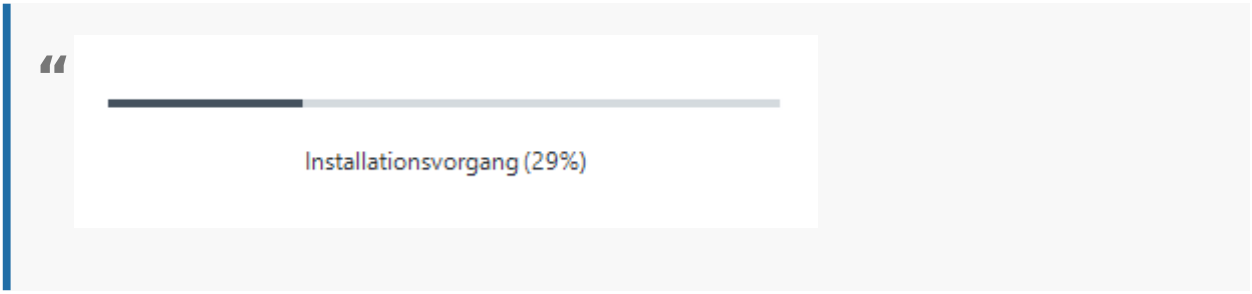


11. Die Installation beginnt mit dem Herunterladen der zum System passenden Installationsdatei.

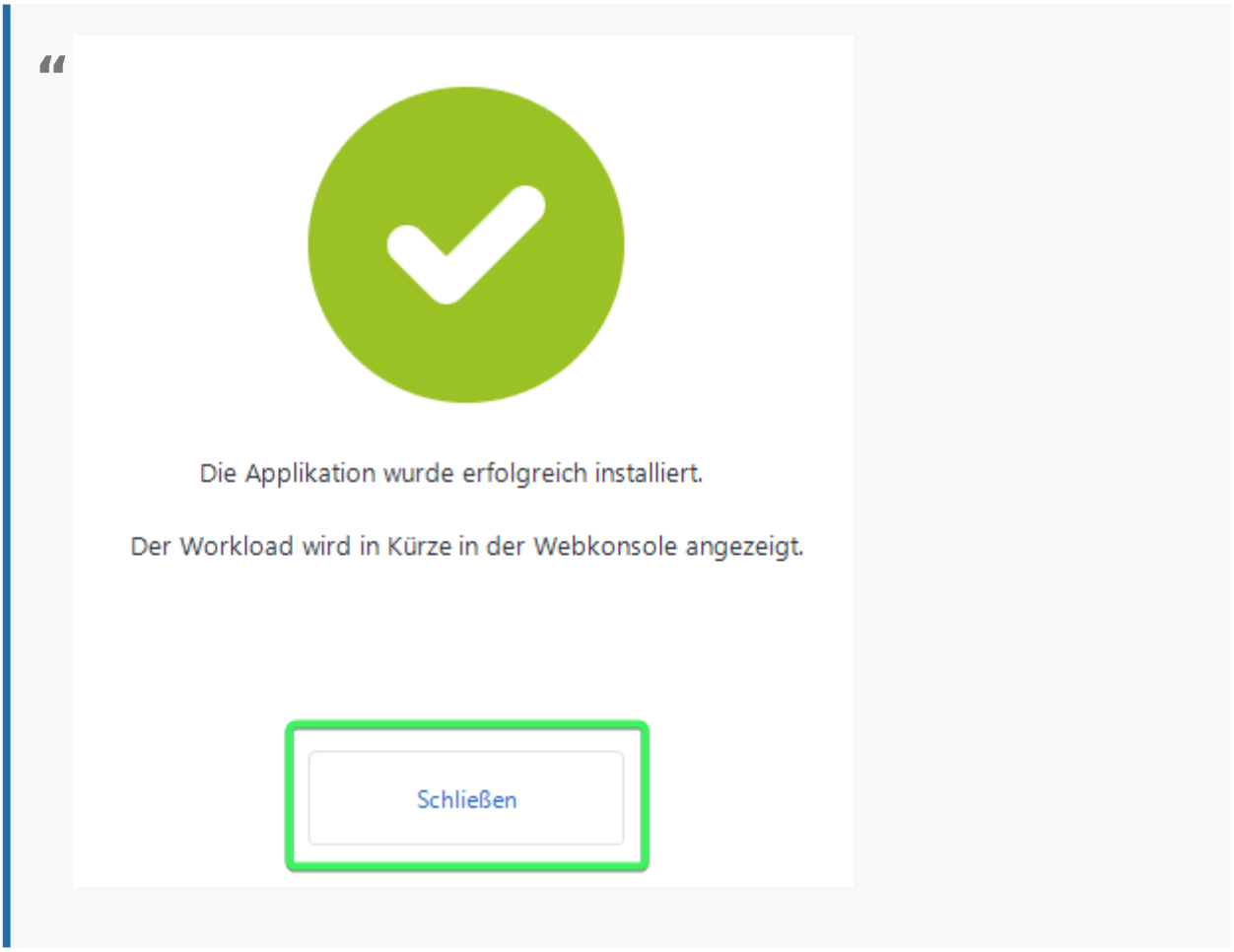


Hinweis Je nach Internet-/Netzwerkanbindung kann dieser Schritt etwas Zeit in Anspruch nehmen.

12. Nach dem Herunterladen beginnt sofort die Installation.



13. Die erfolgreiche Installation wird angezeigt und kann mit **„Schließen"** verlassen werden.



14. Informieren Sie das Team der CSG, sobald die Installation auf dem/den System(en) abgeschlossen ist, und auf welchen Systemen Sie dies abgeschlossen haben.

Kurze Checkliste

- Downloadlink und Registrierungs-Token vom CSG-Team erhalten?
- Installation mit Administratorrechten und „Als Administrator ausführen" gestartet?
- Bei den Installationseinstellungen **ausschließlich** die Registrierungseinstellungen geändert?
- Registrierungstoken korrekt eingetragen und bestätigt?
- Installation erfolgreich abgeschlossen?
- CSG-Team über abgeschlossene Installation und betroffene Systeme informiert?

FAQ – kurz & knapp

- Wie lange ist das Registrierungstoken gültig?
  - Im Regelfall einen Tag – die Installation sollte daher zeitnah nach Erhalt des Tokens durchgeführt werden.
- Darf ich bei den Installationseinstellungen auch andere Optionen anpassen?
  - Nein, es sollten ausschließlich die Registrierungseinstellungen geändert werden – alle anderen Einstellungen bitte unverändert lassen.

- Was mache ich, wenn die Installation abgeschlossen ist?
  - Informieren Sie das CSG-Team darüber, dass die Installation abgeschlossen ist und auf welchen Systemen dies erfolgt ist.

Fußzeile
Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: https://csg.gmbh/faq-acp-agent-installation

E-Mail-Sicherheit / HornetSecurity / Security Awareness Service / Ablauf und Reaktionen

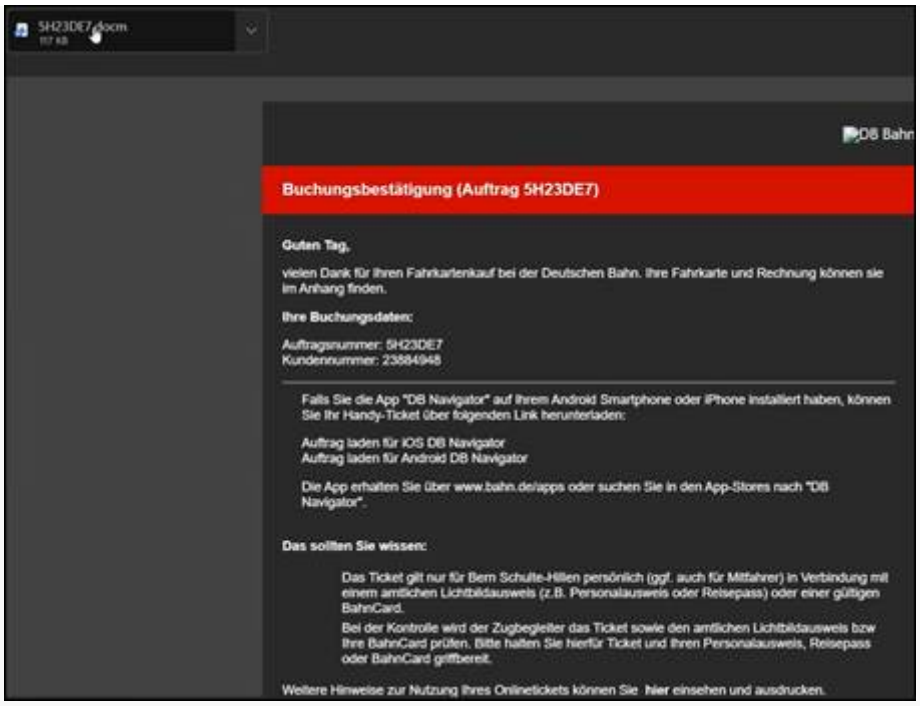
Kurzbeschreibung: Was passiert beim aktivierten Security Awareness Service, wenn eine simulierte Phishing-E-Mail zugestellt wird? Dieser Artikel erklärt den Ablauf, die verschiedenen Reaktionsmöglichkeiten und wie sich das persönliche Level dadurch verändert.

Für wen relevant?

- Alle Mitarbeiter, deren Postfach über den HornetSecurity Security Awareness Service abgesichert wird und die simulierte Phishing-Mails erhalten.

Kurze Erklärung – Wie funktioniert der Security Awareness Service?

- Der Security Awareness Service arbeitet mit verschiedenen **Leveln**. Jeder Benutzer beginnt in Level 1, dem niedrigsten Level, und steigt oder fällt je nach Reaktion auf simulierte Phishing-E-Mails.
- Ein Aufstieg ist möglich, wenn verdächtige E-Mails erkannt und über das HornetSecurity-Add-in in Outlook gemeldet werden. Je höher das Level, desto anspruchsvoller werden die simulierten Phishing-Mails.
- Grundlage dafür ist der **Employee Security Index (ESI®)** von HornetSecurity, ein Benchmark, der das Sicherheitsverhalten fortlaufend misst und daraus steuert, welche Trainingsinhalte und wie anspruchsvolle Phishing-Simulationen als Nächstes zugestellt werden.

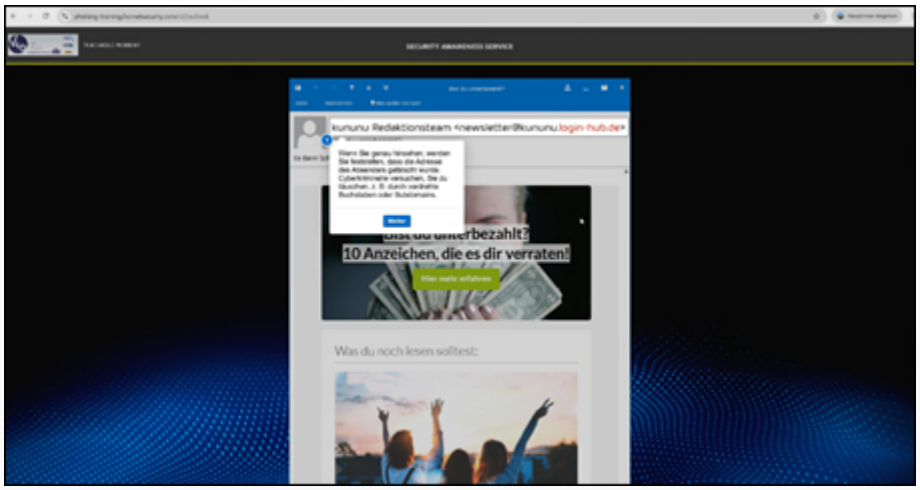


Wie wirken sich verschiedene Reaktionen aus?

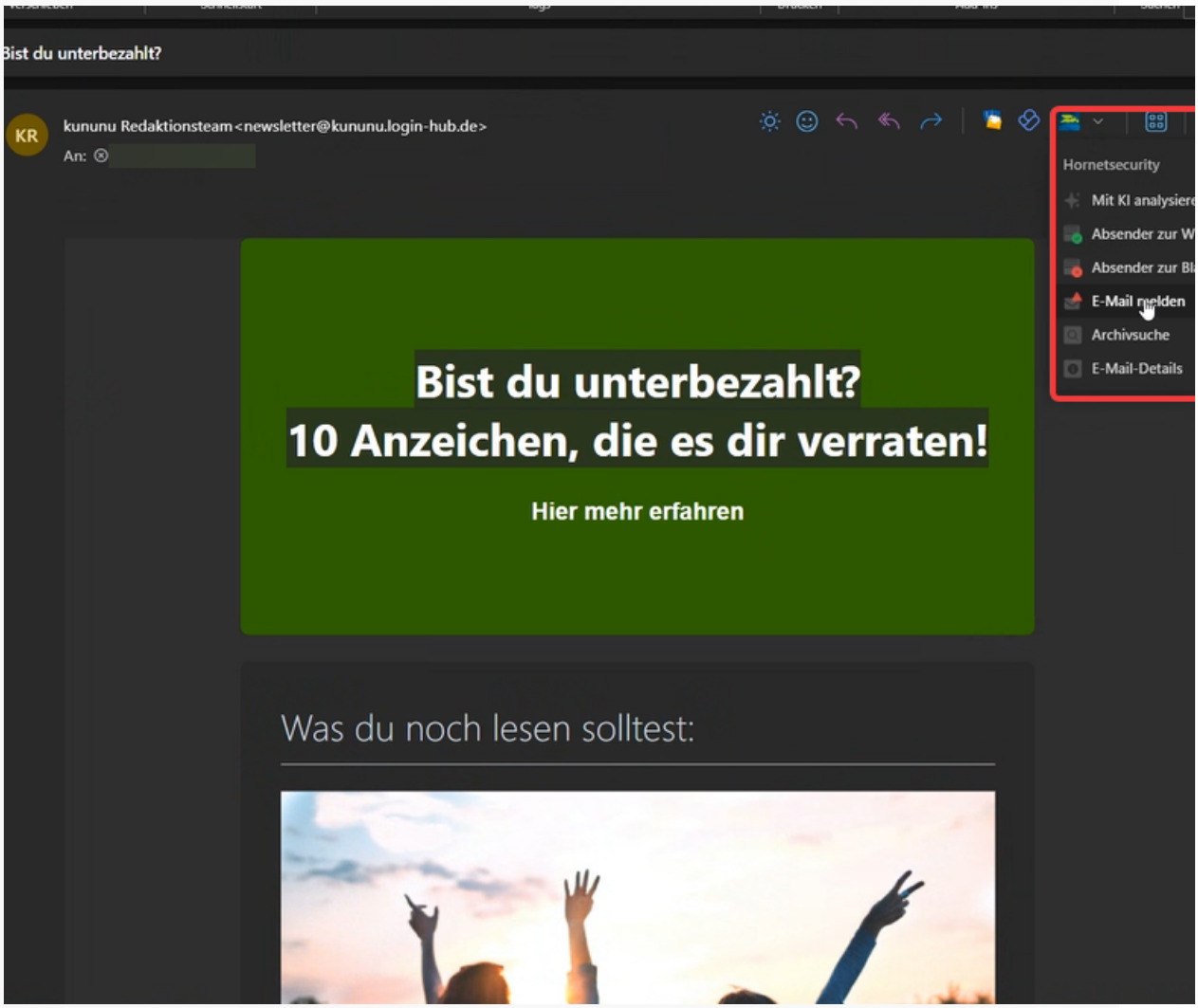
Der Benutzer kann mit der Phishing-E-Mail wie mit jeder E-Mail interagieren – beispielsweise den Anhang öffnen oder auf enthaltene Links klicken.

1. **Interaktion mit der Mail (Anhang öffnen, Link klicken):** Es wird ein Hinweisfenster eingeblendet, das informiert, dass es sich um eine Phishing-Mail handelt.

2. Nach einer solchen Interaktion kann direkt ein sogenannter **Teachable Moment** angezeigt werden. Diese E-Trainings beziehen sich unmittelbar auf die zuvor ausgelöste Phishing-Mail und unterstützen den Lernprozess.



3. **Korrektes Melden:** Alternativ kann die E-Mail über das HornetSecurity-Outlook-Add-in gemeldet werden. Wird eine E-Mail korrekt gemeldet, erhält der Benutzer umgehend eine Rückmeldung.



4. **Ignorieren:** Eine weitere Möglichkeit besteht darin, die E-Mail zu ignorieren.

Hinweis Sowohl durch korrektes Melden als auch durch Ignorieren steigt der Benutzer schrittweise im Level auf. Das Ignorieren der Mails hat jedoch nicht den gewünschten Effekt – erst das aktive Erkennen und Melden trainiert den sicheren Umgang mit echten Phishing-Angriffen nachhaltig.

Achtung Nicht jede Interaktion wird gleich bewertet: Das Öffnen potenziell gefährlicher Inhalte (z. B. eine Makrodatei im Anhang) wird deutlich negativer gewertet als das bloße Öffnen einer E-Mail. Bei schwächerem Sicherheitsverhalten kann das Level daher auch wieder sinken und die Simulationen werden vorübergehend wieder einfacher, bis sich das Verhalten verbessert.

Tipp Verdächtige E-Mails können nicht nur über das Outlook-Add-in gemeldet werden, sondern in vielen Konfigurationen zusätzlich per Weiterleitung an die Adresse `reportto@hornetsecurity.com`. Welcher Weg für Ihr Unternehmen zur Verfügung steht, teilt Ihnen bei Bedarf Ihr IT-Team mit.

Kurze Checkliste

- Wissen, dass alle Benutzer in Level 1 starten und sich das Level durch das eigene Verhalten verändert?
- Bei einer verdächtigen (simulierten) Phishing-Mail: nicht interagieren, sondern über das HornetSecurity-Add-in melden?
- Teachable Moments/E-Trainings nach Interaktion mit einer simulierten Phishing-Mail bewusst durcharbeiten?

- Bewusst, dass reines Ignorieren zwar zum Levelaufstieg beiträgt, aber weniger effektiv trainiert als aktives Melden?

FAQ – kurz & knapp

- Was passiert, wenn ich auf eine simulierte Phishing-Mail hereinfalle?
  - Es erscheint ein Hinweisfenster, das über die Simulation aufklärt, häufig gefolgt von einem kurzen, auf den Vorfall zugeschnittenen E-Training (Teachable Moment).
- Wie steige ich im Level auf?
  - Durch korrektes Erkennen und Melden simulierter Phishing-Mails über das HornetSecurity-Add-in – aber auch durch bloßes Ignorieren steigt das Level, wenn auch mit geringerem Lerneffekt.
- Kann mein Level auch wieder sinken?
  - Ja, insbesondere bei riskanteren Interaktionen wie dem Öffnen potenziell gefährlicher Anhänge wird das Sicherheitsverhalten negativer bewertet, was sich auch auf das Level auswirken kann.
- Was ist der Employee Security Index (ESI®)?
  - Ein von HornetSecurity entwickelter Benchmark, der das Sicherheitsverhalten von Mitarbeitenden fortlaufend misst und daraus ableitet, welche Trainingsinhalte und Phishing-Simulationen als Nächstes sinnvoll sind.

Fußzeile
Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: https://csg.gmbh/faq-hornetsecurity-awareness-ablauf

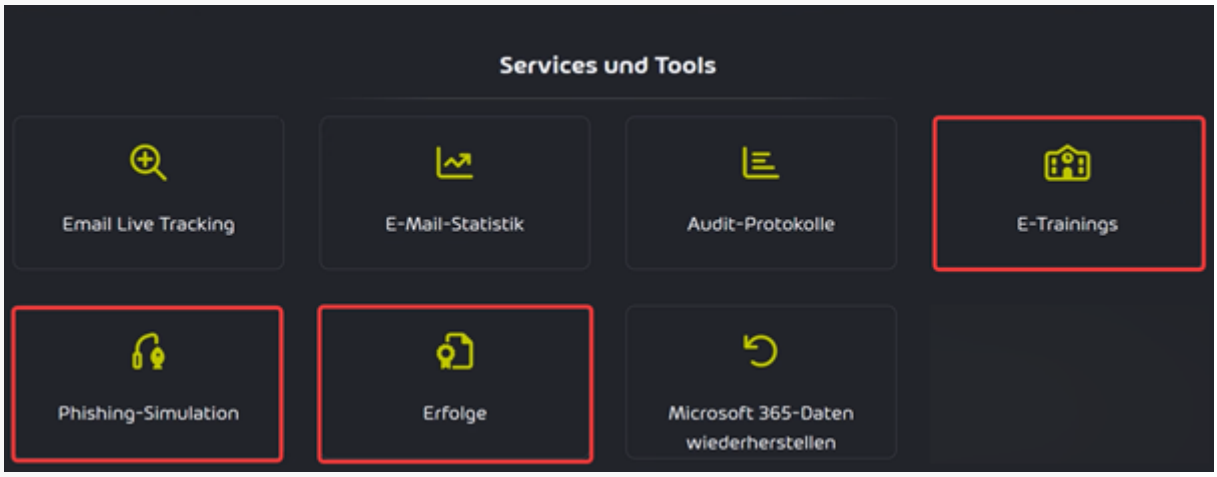
E-Mail-Sicherheit / HornetSecurity / Security Awareness Service / UserPanel

Kurzbeschreibung: Durch das Aktivieren des Features „Security Awareness Service" stehen im UserPanel drei weitere Punkte zur Verfügung: **E-Trainings**, **Phishing-Simulation** und **Erfolge**. Dieser Artikel zeigt, was sich hinter den drei Bereichen verbirgt.

Für wen relevant?

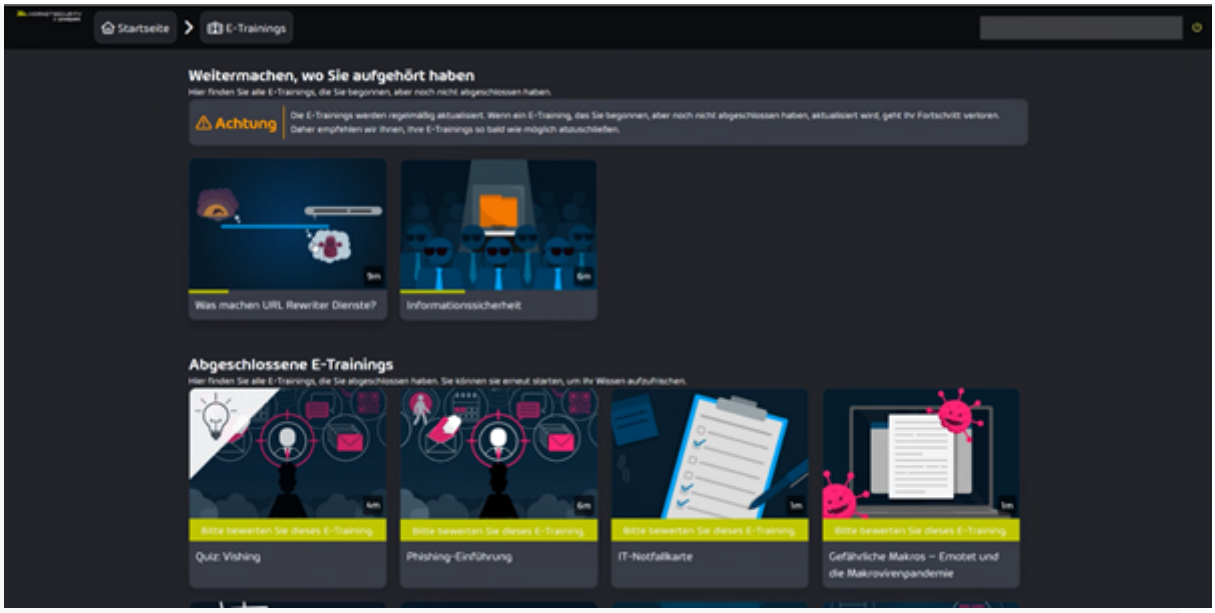
- Alle Benutzer, für die der HornetSecurity Security Awareness Service aktiviert ist und die ihre eigenen Trainings, Statistiken oder Zertifikate im UserPanel einsehen möchten.

Übersicht der drei neuen Bereiche



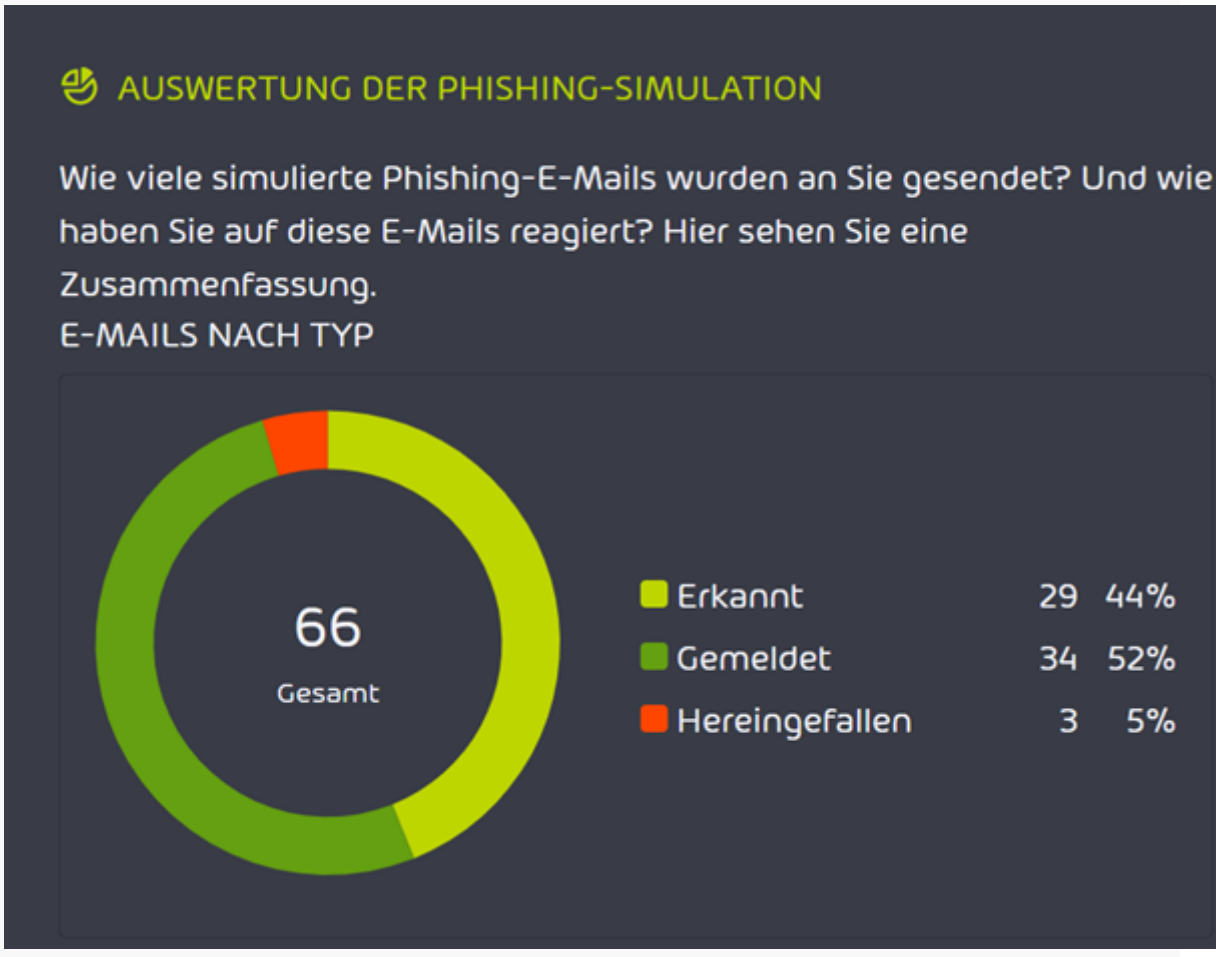
E-Trainings

Unter **E-Trainings** werden alle bisher bestandenen, laufenden und verfügbaren E-Trainings aufgelistet.



Phishing-Simulation

Unter **Phishing-Simulation** wird die eigene Benutzerstatistik und der Verlauf der versendeten simulierten Phishing-E-Mails angezeigt – u. a., ob diese erkannt oder angeklickt wurden.



Hinweis In der Statistik wird zwischen unterschiedlich schwerwiegenden Reaktionen unterschieden: Als **„erkannt"** gelten simulierte Phishing-Mails, bei denen der Angriff nicht erfolgreich war – dazu zählen sowohl korrekt gemeldete als auch ignorierte E-Mails. Bei nicht erkannten E-Mails wird zusätzlich erfasst, wie stark reagiert wurde, z. B. **angeklickte Links**, **eingegebene Zugangsdaten**, **geöffnete Dateien** oder **ausgeführte Makros** – Letzteres wird dabei am schwersten gewertet.

Erfolge

Unter **„Erfolge"** kann sich der Benutzer ein Zertifikat erstellen lassen, das alle bestandenen E-Trainings auflistet.

Tipp Das Zertifikat unter „Erfolge" eignet sich gut als persönlicher Nachweis absolvierter Sicherheitsschulungen, z. B. gegenüber Vorgesetzten oder für die eigene Personalakte.

Kurze Checkliste

- Bereich „E-Trainings" auf offene bzw. verfügbare Trainings geprüft?
- Eigene Statistik unter „Phishing-Simulation" zur Selbsteinschätzung genutzt?
- Bei Bedarf Zertifikat unter „Erfolge" erstellt?

FAQ – kurz & knapp

- Wo finde ich meine offenen E-Trainings?
  - Im UserPanel unter dem Menüpunkt „E-Trainings" – dort werden bestandene, laufende und verfügbare Trainings aufgelistet.
- Was zeigt mir die Statistik unter „Phishing-Simulation" genau?
  - Ihre persönliche Bilanz zu simulierten Phishing-Mails: welche erkannt wurden und – bei nicht erkannten Mails – wie darauf reagiert wurde (z. B. Link angeklickt, Zugangsdaten eingegeben, Datei geöffnet oder Makro ausgeführt).
- Wie bekomme ich einen Nachweis über meine absolvierten Trainings?
  - Über den Bereich „Erfolge" lässt sich ein Zertifikat mit allen bestandenen E-Trainings erstellen.

Fußzeile
Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: https://csg.gmbh/faq-hornetsecurity-awareness-userpanel