Cybersecurity Awareness Study 2020

Höhere Aufmerksamkeit und Sicherheit

www.lucysecurity.com
www.lucysecurity.com/laws

Lucy

INHALT

Der Nutzen von Cyber Security Awareness geht viel weiter als 'nur' besser ausgebildete Mitarbeiter und weniger Sicherheitsvorfälle.

– Palo Stacho Studienleiter LUCY Security

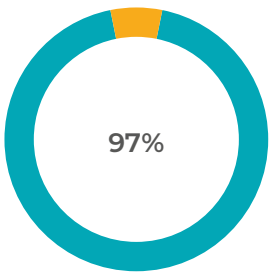
EINLEITUNG

Der Nutzen von Awareness, insbesondere von Phishing Simulationen, wird aktuell in der Öffentlichkeit breit diskutiert. Die Berichterstattung in den Medien zu Hacks bei Unternehmen und über Datenabflüsse gehört inzwischen zum Alltag.

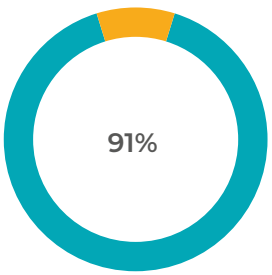
Der sogenannte 'Faktor Mensch' ist im Fadenkreuz der Cyberkriminellen. 97% der Angriffe im Internet zielen auf den Menschen. Lediglich drei Prozent sind gegen die Maschinen gerichtet [1]. Fakt ist auch, dass 91% der erfolgreichen Angriffe durch unachtsame Mitarbeiter eingeleitet werden [2]. Immer mehr Organisationen werden sich diesem Umstand bewusst. Nicht nur Großfirmen sondern der Mittelstand und auch KMU investieren darum heutzutage nicht nur in professionelle IT-Security Lösungen, sondern auch in die Fortbildung ihrer Mitarbeiter, damit sich diese sicherheitsbewusster verhalten. Mitarbeiter im 21. Jahrhundert müssen wissen, welche aktuellen Bedrohungsszenarien aus dem Internet kommen und müssen potentielle Angriffe erkennen können.

Neben klassischer auf Hardware und Systemen basierender IT-Sicherheit verfolgt Cybersecurity Awareness das Ziel zum allgemeinen Schutz des Unternehmens vor den Schäden der Cyberkriminalität. Erreicht wird dies anhand gezielter Schulung der Mitarbeiter. Auch werden dem Mitarbeiter Werkzeuge zur Verfügung gestellt, wie beispielsweise die Möglichkeit, verdächtige Mails zu melden oder analysieren zu lassen. Durch interne Analysen hat Lucy Security festgestellt, dass richtig durchgeführte Awareness-Programme ein Unternehmen bis zu zehnmal sicherer machen. Doch der Nutzen geht erheblich weiter. Haben in der Vergangenheit die Studien eher technische Aspekte von Cybersecurity Awareness und die Stärkung der IT-Sicherheit untersucht, so wurde mit der vorliegenden Studie "Nutzen und Herausforderungen von Cybersecurity Awareness 2020" auch das übergeordnete unternehmensweite Nutzenpotential erforscht.

Der hier vorliegende Bericht zeigt, dass der Einfluss von Cybersecurity Awareness vielfältiger ist als erwartet. Die Wirkung reicht weiter als 'nur' zum besser ausgebildeten Mitarbeiter oder zu weniger Sicherheitsvorfällen. Positive Auswirkungen sind etwa auch bei der Unternehmenskultur und beim Betriebsklima der befragten Unternehmungen erkennbar. Bei den Herausforderungen wird ersichtlich, dass diese nicht nur technischer Natur sind oder das unzureichende Budget betreffen, sondern dass Awareness häufig erhöhte Herausforderungen an die Führung stellt und zudem klar eine Innovationsaufgabe ist. Das Ziel ist schlussendlich die Erreichung eines sicheren Mitarbeiterverhaltens bei der Belegschaft. Effektive und nachhaltige Cybersecurity Awareness betrifft jede Unternehmung! Die Umsetzung war noch nie so einfach wie heute. Heutzutage ist eine beachtliche Menge von Lösungen am Markt erhältlich. Beim Einsatz solcher Produkte und Plattformen sollte man beachten, dass möglichst integrierte Suiten zur Verwendung kommen sollten. Und da Sicherheit eher ein Prozess ist als ein Produkt [3], kommt den Kosten ein besonderes Augenmerk zu. Awareness Maßnahmen gehören neu zum Arbeitsalltag und sind laufend durchzuführen. Ist die Umsetzung kompliziert und teuer, dann wird die Sicherheit der Unternehmung darunter leiden.



> of the Attacks try to trick a user with some social engineering scheme



> of Cyberattacks and the resulting data breach begin with a spear pishing email

DIE WICHTIGSTEN ERGEBNISSE 2020

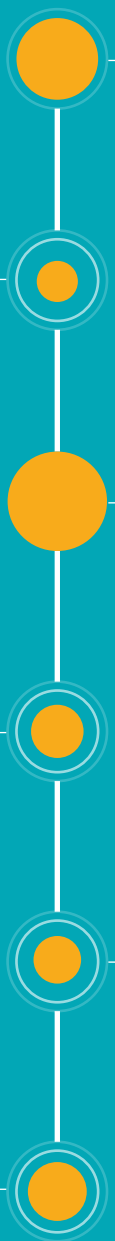
Fast alle der befragten Organisationen haben Cybersecurity Awareness Maßnahmen umgesetzt (96%) und vier von fünf Unternehmungen führen spezielle Phishing Simulationen durch.

Dieses Resultat erstaunt nicht im Anbetracht der international angeschriebenen Zielgruppe von rund 900 IT-Security Professionals. Beachtenswert ist jedoch, dass lediglich ein wenig mehr als die Hälfte der Organisationen ihre Mitarbeiter in ihr Sicherheitsdispositiv einbindet: 51% der Unternehmungen haben einen 'Phishing Incident Button' in Verwendung. Sie aktiveren damit einerseits den 'Human Firewall' und andererseits gibt man dem verunsicherten Mitarbeiter ein simples aber mächtiges Werkzeug in die Hände, das im täglichen Umgang mit Emails einen grossen Rückhalt bietet.

Cybersecurity Awareness hat einen weit über IT-Sicherheit reichenden Gesamtnutzen für die Unternehmung: Alle (!) Befragten der Studie geben an, dass Security Awareness sich positiv auf die Fehlerkultur des Unternehmens auswirkt. Weiter geben 89% der Organisationen an, dass die Maßnahmen das Vertrauen in die Geschäftsleitung gestärkt haben. Das bedeutet, dass in den Unternehmen bei den Mitarbeitern eine sehr hohe Akzeptanz für Security Awareness besteht und dem Management zugestanden wird, hier etwas richtiges und nützliches zu tun. So erstaunt es auch nicht, dass fast drei Viertel der Unternehmen angeben, dass die durchgeführten Awareness Maßnahmen keine Ängste bei ihren Angestellten auslösen. Die obigen Resultate lassen den Schluss zu, dass Cybersecurity Awareness einen hohen Beitrag zur allgemeinen Unternehmenssicherheit leistet und direkte positive Effekte bei Betriebsklima und Firmenkultur erzeugt. Daher ist es nur richtig und von strategischer Bedeutung, dass 92% der Studienteilnehmer angeben, dass das Sicherheitsniveau nicht gehalten werden kann, wenn man nur technische Sicherheitsmaßnahmen ohne Security Awareness umsetzt. Die oft verwendeten ISO-Normen [4] oder das NIST-Rahmenwerk [5] greifen im Bereich von Awareness zu kurz. Eine prominente Verankerung von Cybersecurity Awareness in der IT-Strategie ist somit ein Muss!

Kein Thema ohne Herausforderungen: Als größte Herausforderungen werden die Erreichung der Benutzerakzeptanz, fehlende Ressourcen (Personal, Zeit, Geld) und die Sicherstellung der Reichweite genannt. Danach folgen fehlender Managementsupport, die Sicherstellung der Effektivität und die Herausforderung beim Management des Wandels.

KEY FINDINGS AUF EINEN BLICK



96%
führen Cyber Security Awareness Maßnahmen durch.

51%
bieten ihren Mitarbeitern einen «Phishing-Button» an.

100%
erkennen durch die Maßnahmen einen positiven Beitrag zur Fehlerkultur des Unternehmens.

89%
Organisationen geben an, dass Cyber Security Awareness das Vertrauen in die Geschäftsleitung stärkt.

73%
geben an, dass durch die Maßnahmen bei den Mitarbeitern keine Ängste ausgelöst haben.

92%
der Teilnehmer geben an, dass das Sicherheitsniveau nicht gehalten werden kann, wenn man nur auf Technik setzt.

Source: LUCY Cybersecurity Awareness Survey 2020

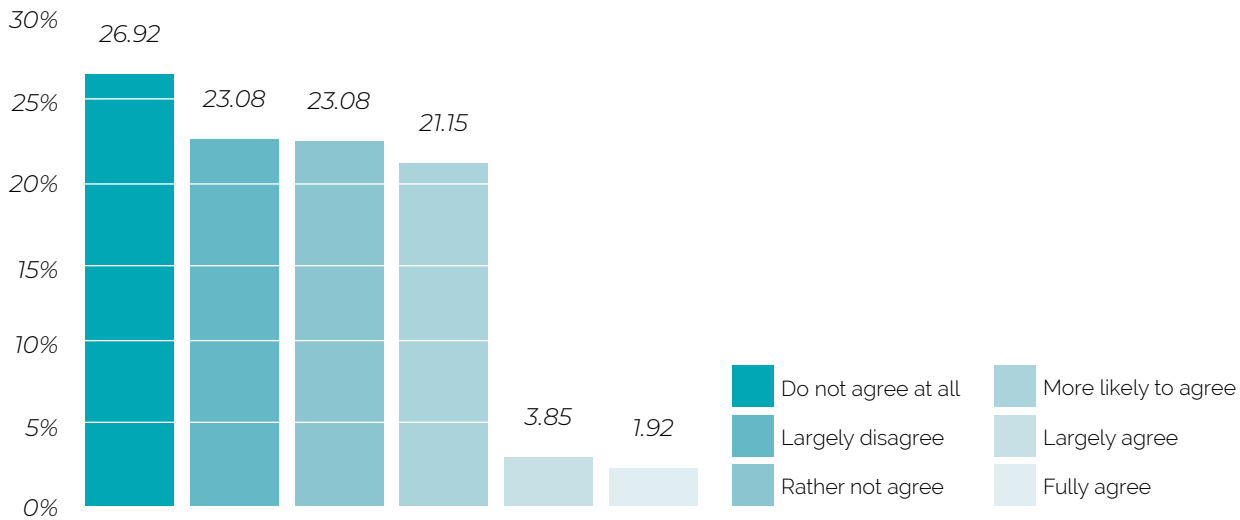
ERGEBNISSE IM DETAIL

Die Umfrageresultate sprechen eine deutliche Sprache: Der positive Beitrag von Cyber Security Awareness geht über die Verbesserung der allgemeinen Unternehmenssicherheit hinaus:

- *Bei allen (100%) Unternehmen führt Cyber Security Awareness zur Verbesserung der Fehlerkultur.*
- *95% der Organisationen konnten mit Security Awareness das Betriebsklima verbessern.*
- *89% geben an, dass Awareness Maßnahmen das Vertrauen in die Geschäftsleitung gestärkt haben.*
- *73% geben an, dass die Awareness Maßnahmen keine Ängste bei der Belegschaft ausgelöst haben.*

Mit einem Anteil von fast drei Vierteln 'Nein'-Antworten wurde zwar die Annahme widerlegt, dass Cyber Security Awareness Maßnahmen Ängste bei der Belegschaft auslöst. Doch die Tatsache, dass ein relevanter Anteil von 27% der Antworten auf Ängste beim Personalkörper hinweist, verdient eine nähere Betrachtung: Die Daten zeigen, dass die bei den Organisationen entstandenen Ängste weitgehend moderater Natur waren. Nur knapp 6% der Antworten zeigen ein hohes Rating bezüglich der Auslösung von Ängsten.

The security awareness have triggered fears among the workface

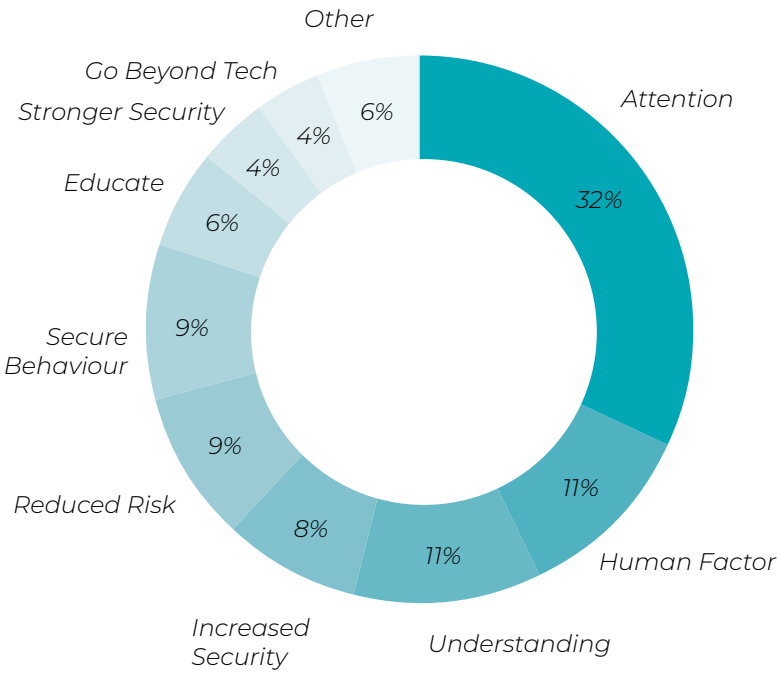


Source: LUCY Cybersecurity Awareness Survey 2020

Major Benefits with Cybersecurity Awareness

AUSWERTUNG

Die Auswertung der freien Antworten zum individuellen Nutzens brachte verschiedene Themencluster zu Tage. Knapp ein Drittel der Organisationen nennen die Aufrechterhaltung der Aufmerksamkeit als Topnutzen (32%). Es folgt mit 11% die Aktivierung des 'Human Factor'. Darunter versteht man die Einbindung und das Engagement des Mitarbeiters in die Alarmierungskette der Unternehmung bei potentiellen Sicherheitsvorfällen. Auf ebenfalls 11% kommt beim Topnutzen die Erreichung des Verständnisses der Belegschaft gegenüber Cyberrisiken. Weitere relevante Nutzencluster sind: Erhöhte IT-Sicherheit, respektive tiefere Security Risiken, die Erlangung eines sicheren Verhaltens der Mitarbeiter, die Schulung der Mitarbeiter, eine stärke IT-Sicherheit oder Maßnahmen, die dort anfangen wo die Technologie aufhört (beim Menschen). Nachfolgend einige ausgewählte Antworten zur Frage «Was ist aus Ihrer Sicht der grösste Nutzen von Cybersecurity Awareness?»



Source: LUCY Cybersecurity Awareness Survey 2020

CLUSTER HUMAN FACTOR

- *«Der schwächste Faktor in der Kette von Maßnahmen - der Mensch - wird gestärkt.»*
- *«Auslastung, Nutzbarmachung der Mitarbeiter.»*
- *«Der Faktor Mensch, die Aufmerksamkeit wird verbessert und die Angriffsfläche verringert.»*

CLUSTER VERSTÄNDNIS

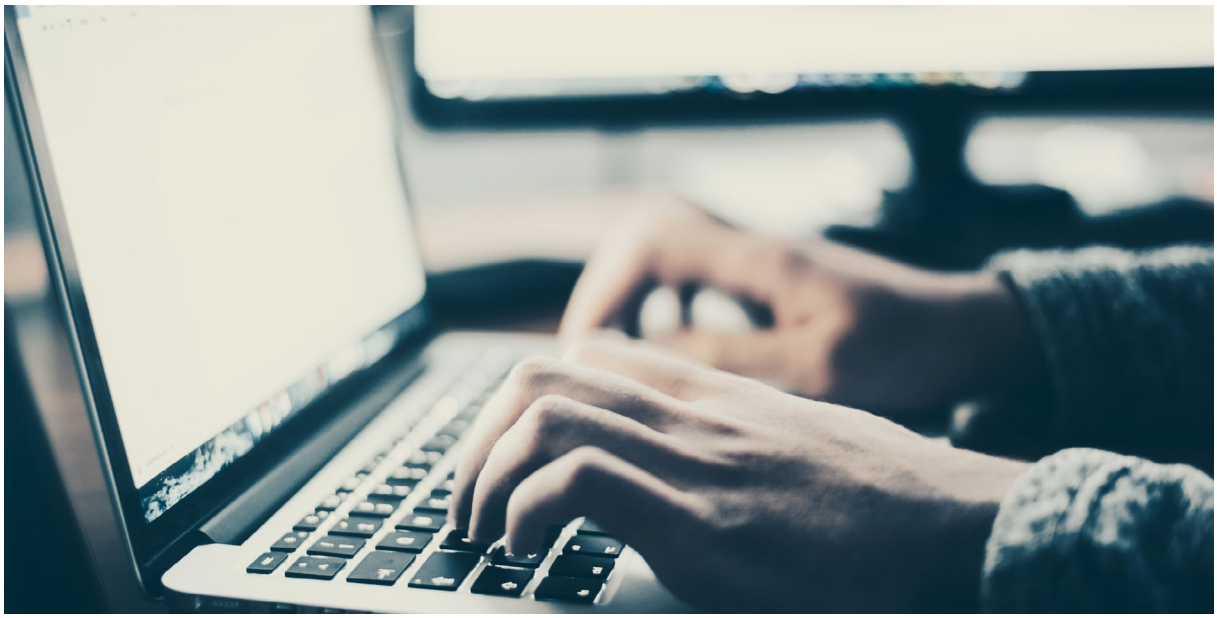
- *«Verständnis der Mitarbeiter für Informationssicherheit.»*
- *«Das Bewusstsein der Kollegen*innen, dass es Cyber Angriffe gibt und wie Sie richtig reagieren, wenn Sie betroffen sind.»*
- *«Das Bewusst-Werden, dass es jederzeit möglich ist, gephisht zu werden.»*

ANDERE (OTHER)

- *«Security wird sichtbar!»*
- *«Weniger Incidents, Integration der Mitarbeiter.»*
- *«Einfacheres Vorgehen durch die Verfügbarkeit vieler Vorlagen.»*

HERAUSFORDERUNGEN

Geht es um die Umsetzung von Cyber Security Awareness Maßnahmen, werden drei Klassen von Herausforderungen erkennbar.



TOPKLASSE

Zur Topklasse zählen der Kampf um die **Benutzerakzeptanz, das Ringen um Ressourcen (Budget, Zeit) und das Erlangen von Reichweite genannt.** Reichweite bezeichnet das Bestreben, möglichst viele Kollegen*innen zu erreichen und abzuholen.

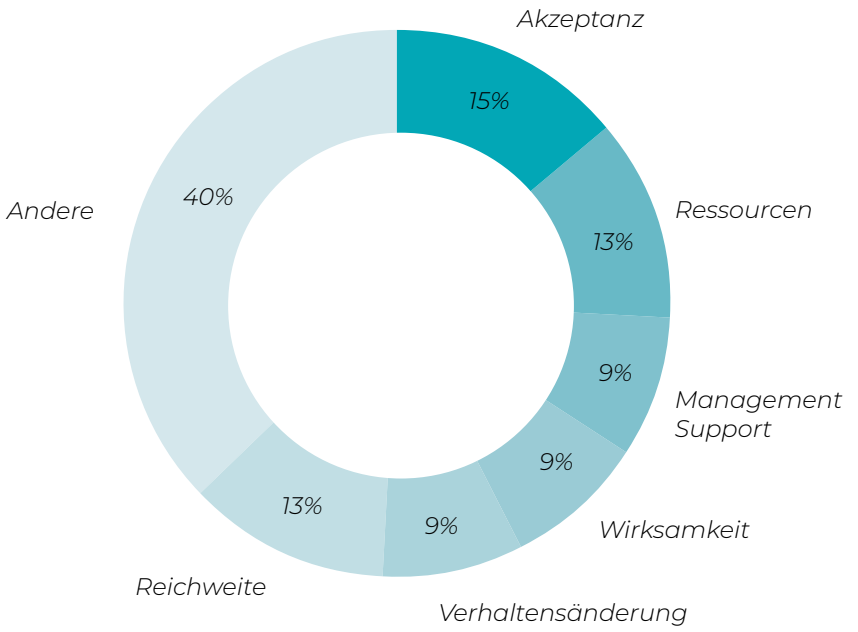
ZWEITE KLASSE

Die zweite Klasse der Herausforderungen ist das Erlangen von Management Support, eine effektive Umsetzung und die Bewältigung des angestrebten Wandels. Bei der Effektivität geht es hauptsächlich darum, das Trainingsangebot richtig auszugestalten, dass die notwendigen Themen gezielt und empfängergerecht geschult werden oder dass das Thema bei den Mitarbeitern langfristig relevant bleibt. Bei der Bewältigung des Wandels dem Behaviour Change bei der Belegschaft hin zum sicheren Verhalten jedes einzelnen Mitarbeiters - sind es Herausforderungen wie die Langwierigkeit des Prozesses. Auch die Motivation von gleichgültigen Mitarbeitern, der Umgang mit der Unwissenheit der Mitarbeiter werden dabei genannt.

DRITTE KLASSE

Zur dritten Klasse gehören alle anderen Herausforderungen verschiedenster Art. Nachfolgend ausgewählte Antworten zur Frage «Was ist aus Ihrer Sicht der grösste Herausforderung von Cybersecurity Awareness?» der Klasse ‚Andere' (Other):

Major Challenges with Cybersecurity Awareness



Source: LUCY Cybersecurity Awareness Survey 2020

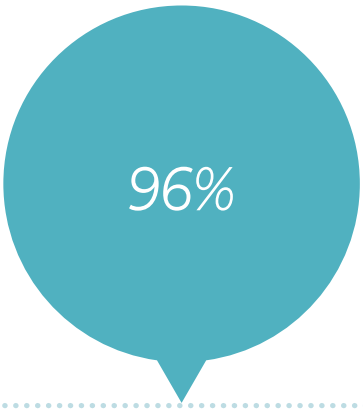
ANTWORTEN ZU DER KLASSE ‚Andere' (Other):

- *„Realitätsnah zu bleiben denn Hacker halten sich an keine Vorgaben."*
- *„Anpassung auf tatsächlich aktuelle Bedrohungen."*
- *„Die bösen Jungs werden immer besser."*
- *„Awareness in den Arbeitsalltag der Mitarbeiter einbauen."*
- *„Mit abwechslungsreichen Kampagnen dafür zu sorgen, dass Mitarbeiter nicht ‚abstumpfen'."*
- *„Der Mensch / Mitarbeiter ist oft das schwächste Glied der Kette, Cyber Angriffe werden immer stärker. Die Zahl nimmt zu und die Attacken werden ausgefeilter."*
- *„Die Sensibilität aktiv zu halten."*
- *„Die Mitarbeiter dazu zu bringen, 'freiwillig' an Schulungen etc. teilzunehmen."*
- *„Die Nützlichkeit herauszustellen und gegen ‚das macht doch die Firewall' anzukämpfen."*
- *„Lösungen müssen customized werden, da die Angebote "von der Stange" nicht zufriedenstellend aufbereitet sind."*
- *„Dass nicht zu viele Simulationen durchgeführt werden."*
- *„Ständiges Balancieren zwischen Realität und Praktikabilität (der Kampagnen und Szenarien)."*
- *„Die Präzision der Tests und die Regelmäßigkeit der Tests."*
- *„Das Filtern und Segmentieren nach Benutzergruppen oder –Klassen."*
- *„Dass Mitarbeiter keine Zeit haben/ wenig Zeit eingeräumt wird für Schulung."*
- *„Die schwächsten Leute zu schulen (top worst)."*

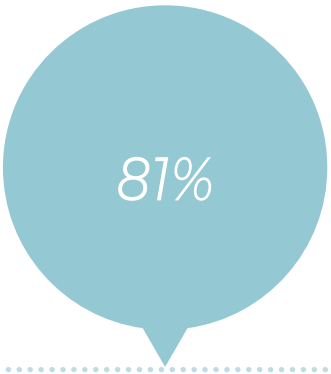
EINSATZ VON CYBER SECURITY

Die Studie hat die im Markt anerkannten Erkenntnisse zur grundsätzlichen Relevanz von Security Awareness bestätigt.

Beachtenswert ist, dass fast die Hälfte der Organisationen darauf verzichtet, den Mitarbeiter in ihr Sicherheitsdispositiv einzubinden: 49% der Unternehmungen haben keinen 'Phishing Button' im Einsatz. Diese Unternehmungen schöpfen das Potential Ihres Personalkörpers nicht aus. Der ‚Human Firewall' wird nicht aktiviert. Obendrein ist der Phishing Alarm Knopf eine nützliche Hilfe, speziell für Mitarbeiter, die im täglichen Umgang mit Emails auf verdächtige Nachrichten stoßen und über deren Legitimität verunsichert sind. So ein „Phish Button" bietet in solchen Situationen einen großen Rückhalt.



aller befragten Organisationen führen Awareness Trainings durch



aller befragten Organisationen führen Phishing Simulationen durch

Source: LUCY Cybersecurity Awareness Survey 2020

Die fehlende Verwendung eines Phishing Incident Buttons verschenkt viel Schutzpotential und Benutzermotivation“.

– Palo Stacho Studienleiter LUCY Security

60%

der befragten Organisationen verwenden LUCY Software

51%

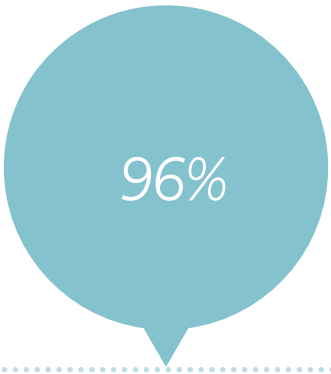
der Organisationen haben einen ‚Phishing Alarm Button’ im Einsatz

UNTERNEHMENSSICHERHEIT UND CYBERSECURITY AWARENESS

UNTERNEHMENSSICHERHEIT

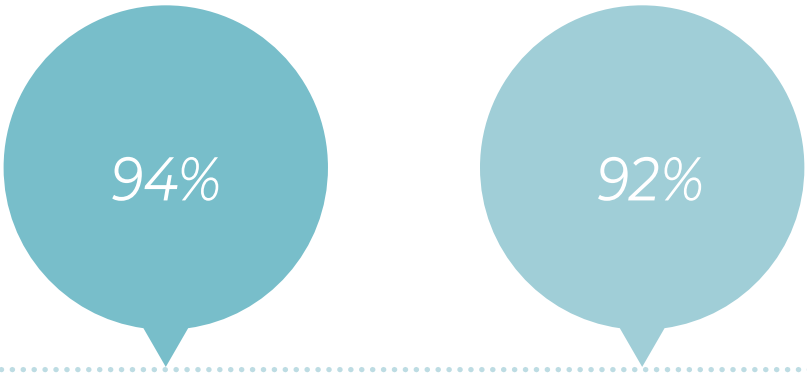
Es wird bestätigt, dass Cybersecurity Awareness die Aufmerksamkeit erhöht und zur Unternehmenssicherheit beiträgt. Gleichzeitig werden Behauptungen widerlegt, dass die Durchführung von Pishing Simulationen die Sicherheits-infrastruktur schwächt, weil sogenannte Whitelistings [6] und ähnliches zur Durchführung eingerichtet werden müssen.

sind überzeugt an, dass Security Awareness Maßnahmen echte Angriffe erschweren.



geben an, dass bei ihnen die Security Awareness zugenommen hat.

Source: LUCY Cybersecurity Awareness Survey 2020



äußern, dass durch Cyber Security Awareness die IT-Sicherheitsinfrastruktur NICHT geschwächt wird.

geben an, dass bei ihnen die Security Awareness zugenommen hat.

CYBERSECURITY AWARENESS UND SICHERHEITS-STRATEGIE

92% der Organisationen glauben, dass das Sicherheitsniveau nicht gehalten werden kann, wenn man nur technische Sicherheits-Maßnahmen umsetzt

Die Industrialisierung der Cyberkriminalität und deren Verbreitung ist ein Phänomen, welches häufig jünger ist als die meisten Security Policies und IT-Strategien, die in den Unternehmungen im Einsatz sind. Natürlich werden solche Reglemente in der Regel laufend aktualisiert. Der Punkt ist aber, dass die Normen, auf welchen solche Policies basieren weit weniger häufig überarbeitet werden.
Die letzte Überarbeitung der ISO27001 Richtlinie datiert zurück ins Jahr 2013[4]. Ein anderes relevantes Rahmenwerk, das NIST Cybersecurity Framework 1.1 ist bedeutend jünger, nämlich von 2018. Doch leider ist auch diese verhältnismäßig junge Norm von der Realität überholt worden. Schon nur durch die zwischenzeitliche Einführung von GDPR[7] und CCPA[8] sind diese Normen aus Awareness-Optik nicht mehr zeitgemäß. Das gilt insbesondere für Unternehmungen, die kritische Infrastrukturen betreiben. Die heute anerkannten Standards ISO27001 und NIST Cybersecurity Framework 1.1 tragen der Notwendigkeit von Cybersecurity Awareness zu wenig Rechnung. Als Folge davon fristet bei vielen IT-Security Strategien der Unternehmen das Thema Cybersecurity Awareness heute (noch) ein Schattendasein. Cybersecurity Awareness nimmt heute eine tragende Rolle bei der Informationssicherheit und beim Unternehmensschutz ein. Ohne Awareness und sensibilisierte Mitarbeiter sind die Organisationen weniger sicher. Awareness Trainings und Phishingsimulationen müssen zwingend in der Sicherheits-Strategie verankert werden.

„In heutigen Standards ISO27001 und NIST Cybersecurity Framework wird dem Thema Cybersecurity Awareness zu wenig Rechnung getragen. Das Resultat ist, dass Awareness in den Security-Strategien der Unternehmen oft wenig Berücksichtigung findet

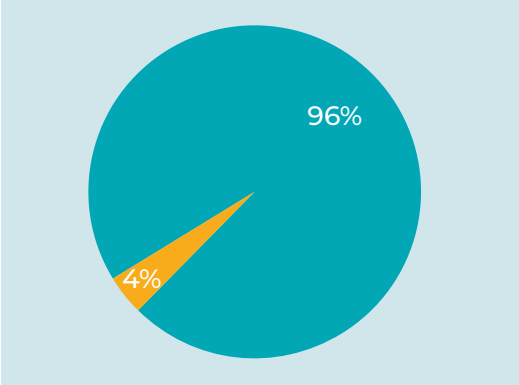
– Patrick Hamilton
Studienmitarbeiter
LUCY Security

FAZIT

91% der erfolgreichen Internetangriffe beginnen beim Mitarbeiter. Mit Cybersecurity Awareness Maßnahmen setzt man genau dort an, nämlich beim Menschen. Die Studie zeigt, dass im Unternehmen damit erhöhte Sensibilisierung und IT-Sicherheit erreicht wird.

Eine Unternehmung hat ohne laufende Cybersecurity Awareness Programme [9] ein tieferes Sicherheitsniveau als mit Awareness Trainings und Phishing Simulationen. Nur die Hälfte der Befragten setzt heute (2020) einen Phishing Incident Button ein und verschenkt dadurch Mitarbeiterengagement und damit Schutzpotential. Alle Studienteilnehmer berichten von einer Verbesserung der Fehlerkultur und 95% bestätigen ein besseres Betriebsklima dank Cybersecurity Awareness. Cybersecurity Awareness Maßnahmen stärken das Vertrauen in die Geschäftsleitung. Der Größte Nutzen wird bei der Sicherheit, Aufmerksamkeit, bei der Stärkung des Faktors Mensch und beim Verständnis für Cybersecurity und Internetbedrohungen erzielt. Die größten Herausforderungen sind die Erreichung der Benutzerakzeptanz, fehlende Ressourcen (Personal, Zeit, Geld) und die Sicherstellung der Reichweite. Danach folgen die Sicherstellung des Managementsupports, Effektivitätsissues und die Herausforderung beim Management des Wandels. Phishing Simulationen und Awareness Trainings sind in der IT-Sicherheitsstrategie zu verankern. Und nicht zu unterschätzen: Cybersecurity Awareness macht Informationssicherheit und die Bemühungen drum herum im Unternehmen sichtbar.

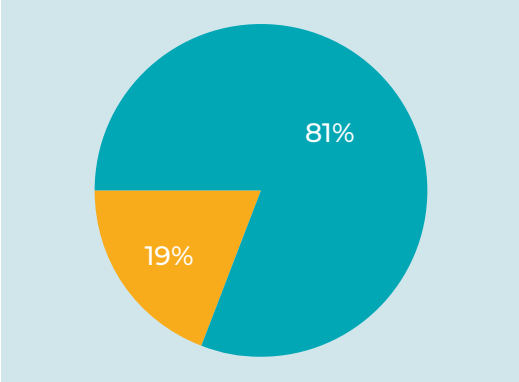
ABBILDUNGEN & TABELLEN



Unsere Organisation führt Awareness Trainings durch

96% Ja
4% Nein

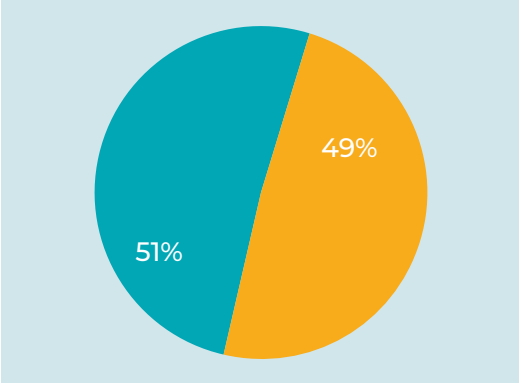
Source: LUCY Cybersecurity Awareness Survey 2020



Unsere Organisation führt Phishing Simulationen durch

81% Ja
19% Nein

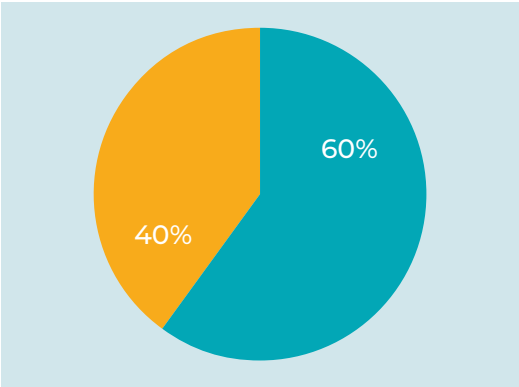
Source: LUCY Cybersecurity Awareness Survey 2020



Unsere Organisation nutzt einen Phishing-Alarm Button oder ähnlich

51% Ja
49% Nein

Source: LUCY Cybersecurity Awareness Survey 2020

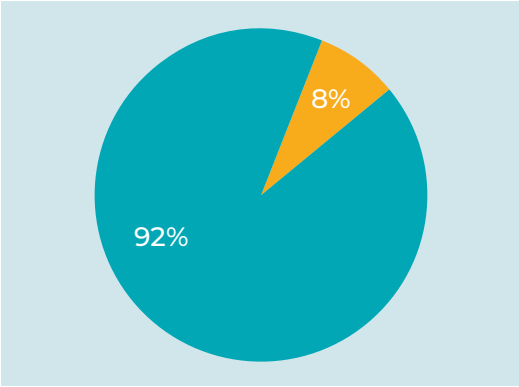


Unsere Organisation verwendet LUCY Software für Cyber Security Awareness

60% Ja

40% Nein

Source: LUCY Cybersecurity Awareness Survey 2020



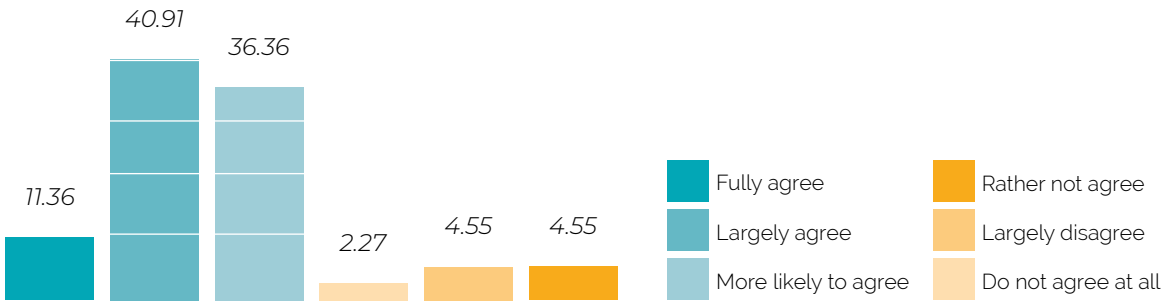
Die Cyber Security Awareness hat in unserer Organisation in den letzten Jahren/Monaten zugenommen

92% Ja

8% Nein

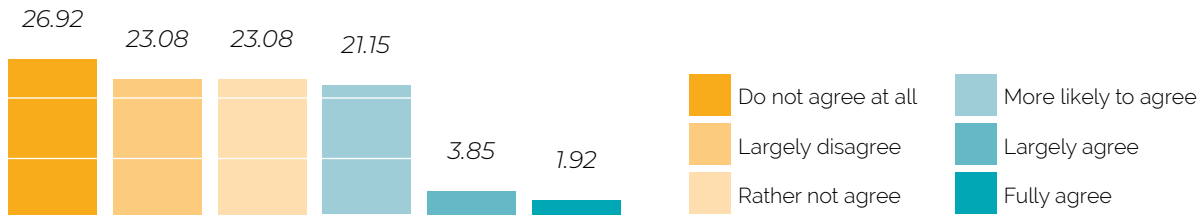
Source: LUCY Cybersecurity Awareness Survey 2020

Das Vertrauen in die Geschäftsleitung wurde durch die durchgeführten Security Awareness Massnahmen gestärkt



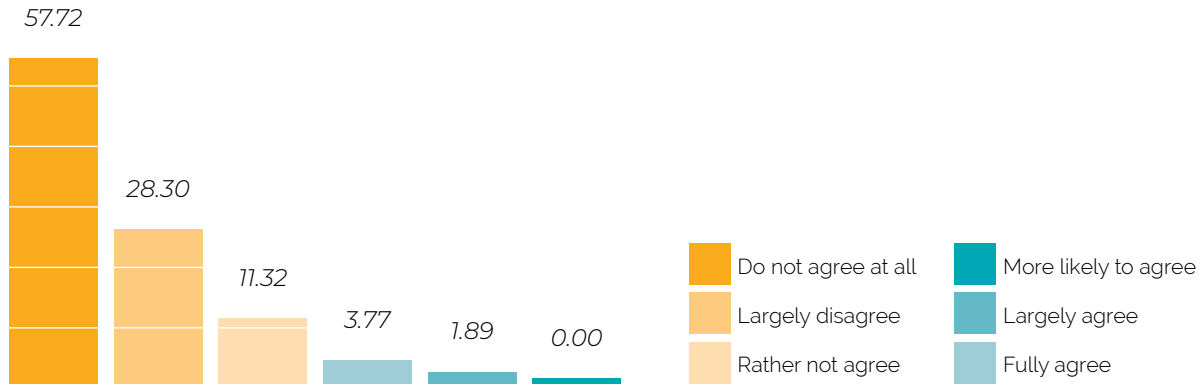
Source: LUCY Cybersecurity Awareness Survey 2020

Die Security Awareness Massnahmen haben bei der Belegschaft Ängste ausgelöst



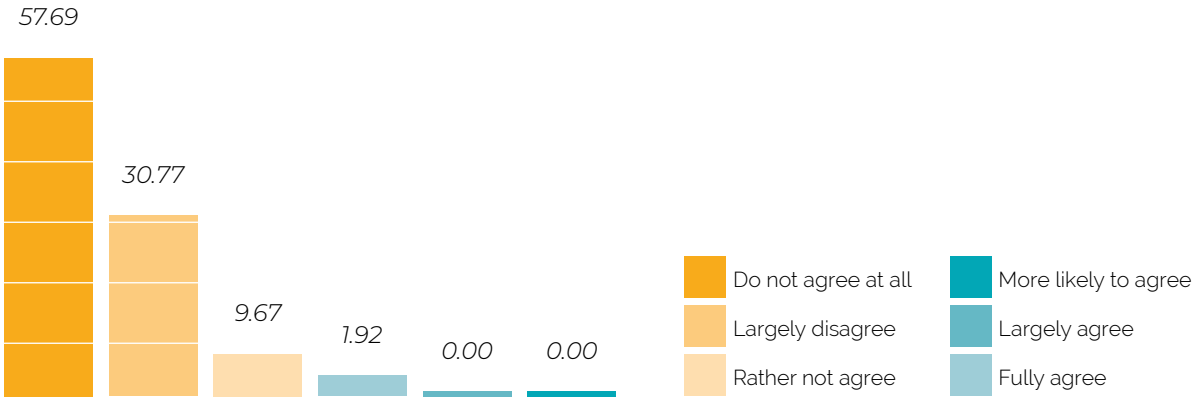
Source: LUCY Cyber Security Awareness Survey 2020

Die Maßnahmen zu Cybersecurity Awareness schwächen die IT-Sicherheitsinfrastruktur des Unternehmens (durch Whitelists, Ausnahmen usw.)



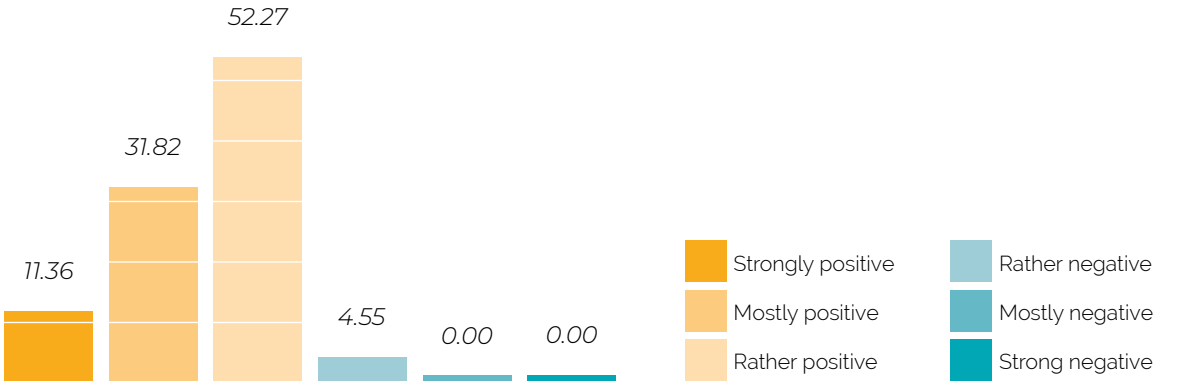
Source: LUCY Cybersecurity Awareness Survey 2020

Die Security Awareness Massnahmen erleichtern es Cyberkriminellen, bösartige Hacking Angriffe durchzuführen (z.B. durch Verwendung von Simulationsvorlagen für echte Angriffe)



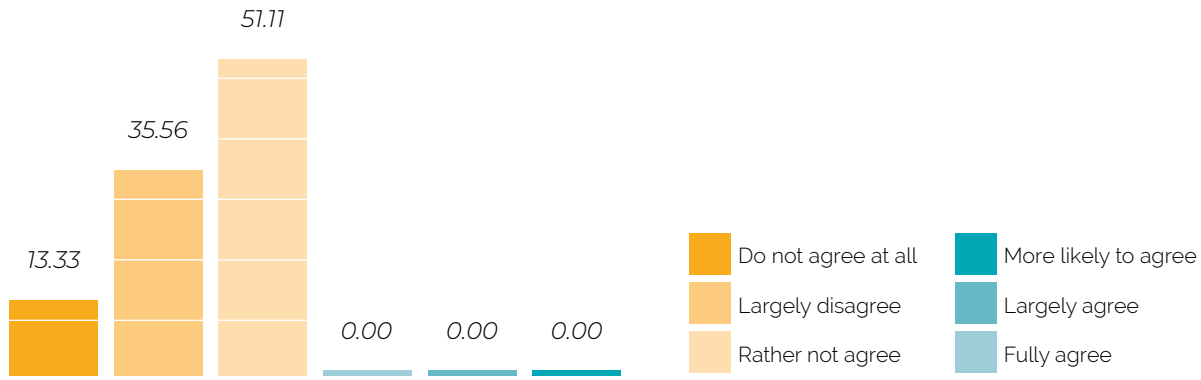
Source: LUCY Cyber Security Awareness Survey 2020

Die Auswirkungen auf das Betriebsklima durch die Phishing Simulationen waren



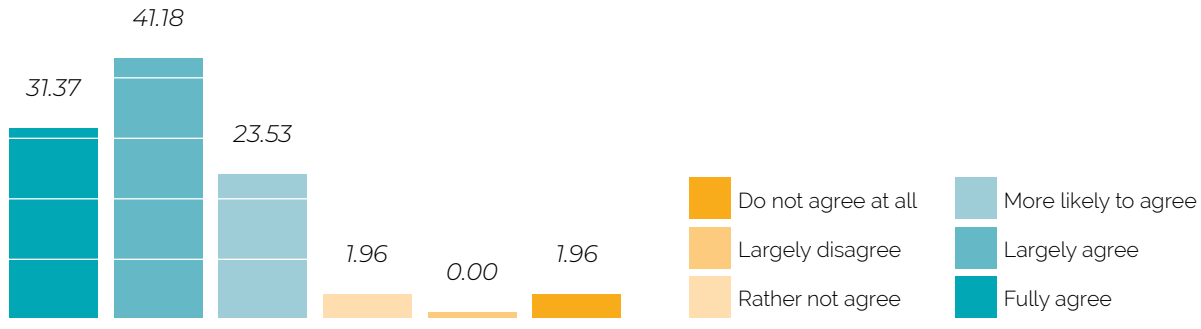
Source: LUCY Cybersecurity Awareness Survey 2020

Der Einfluss der Awareness Massnahmen wirkte auf die Fehlerkultur des Unternehmens

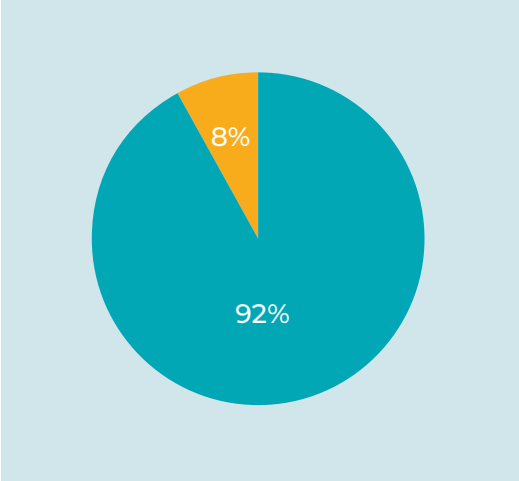


Source: LUCY Cybersecurity Awareness Survey 2020

Cybersecurity Awareness führte zu einem höheren Sicherheitsniveau



Source: LUCY Cybersecurity Awareness Survey 2020



Sind Sie der Meinung, dass ein gleiches IT-Sicherheitsniveau in Ihrer Organisation aufrechterhalten werden kann, wenn die vorhandenen Ressourcen und Gelder ausschliesslich in technische Sicherheits-massnahmen investiert würden (Firewalls, Application Gateways, Virenscanner, Mail-Sandbox Systeme, etc.)?

8% Ja

92% Nein

Source: LUCY Cybersecurity Awareness Survey 2020

Umfrageergebnisse für den Dachraum

32% der Umfrageteilnehmer stammen aus Deutschland, Österreich und der Schweiz. Diese Regionweist leicht andere Studienresultate aus:

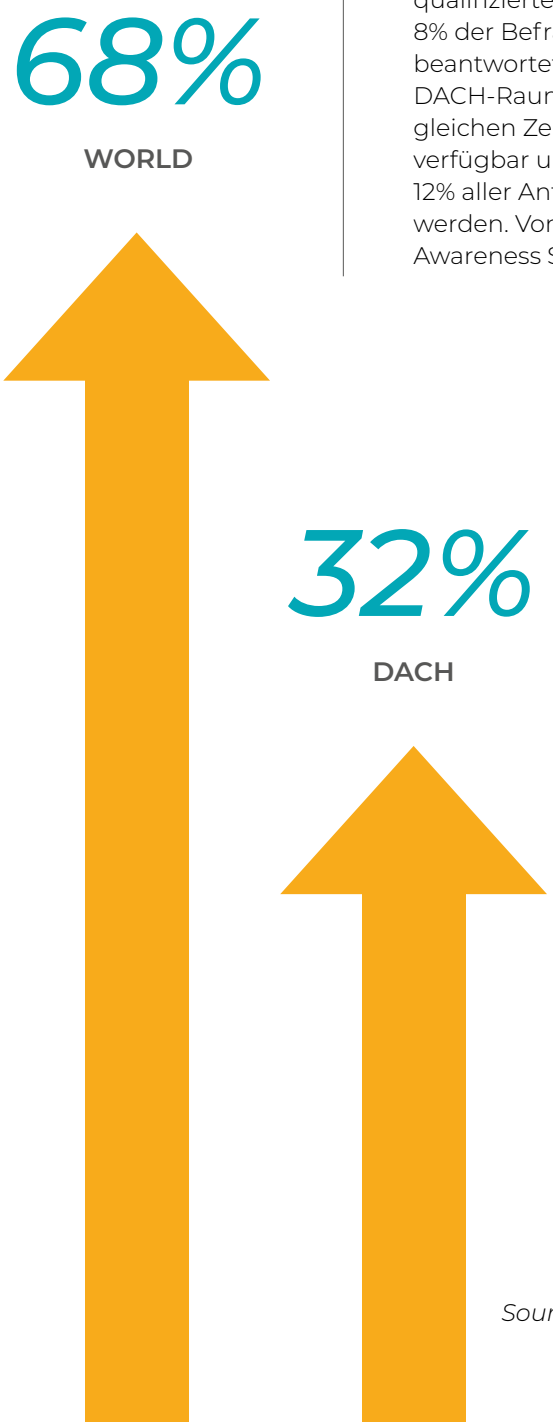
- *Bei allen DACH-Unternehmen führte Cybersecurity Awareness zur Verbesserung der Fehlerkultur.*
- *94% der DACH-Organisationen konnten mit Security Awareness das Betriebsklima verbessern.*
- *91% geben in DACH an, dass Awareness Maßnahmen das Vertrauen in die Geschäftsleitung gestärkt haben.*
- *76% geben in DACH an, dass die Awareness Maßnahmen keine Ängste bei der Belegschaft ausgelöst haben.*
- *96% befragten DACH-Organisationen führen Awareness Trainings durch.*
- *83% der befragten DACH-Organisationen führen Phishing Simulationen durch.*
- *48% der DACH-Organisationen haben einen ‚Phishing Alarm Button' im Einsatz.*
- *63% der befragten DACH-Organisationen verwenden LUCY Software.*
- *90% geben in DACH an, dass bei ihnen die Security Awareness zugenommen hat.*
- *98% geben in DACH an, dass durch Cyber Security Awareness die IT-Sicherheitsinfrastruktur NICHT geschwächt wird.*
- *Alle Umfrageteilnehmer geben in DACH an, dass Security Awareness Maßnahmen echte Angriffe nicht erleichtern.*
- *100% aller Organisationen geben an, dass Security Awareness zu einem höheren Sicherheits-niveau führt.*
- *98% der DACH-Organisationen geben an, dass das Sicherheitsniveau nicht gehalten werden kann, wenn man nur technische Sicherheits Maßnahmen umsetzt.*

Die obigen Resultate waren für die Studienleitung eine Überraschung: Der DACH-Raum als Region ist von Security Awareness gar mehr überzeugt als der Rest der Welt!

METHODOLOGIE

ONLINESTUDIE

Die weltweite Onlinestudie „Nutzen und Herausforderungen von Cybersecurity Awareness 2020“ (“Benefits and challenges of Cybersecurity Awareness 2020”) wurde im Zeitraum vom 25. Juni bis zum 16. Juli 2020 bei knapp 900 qualifizierten Security Spezialisten durchgeführt. Mehr als 8% der Befragten haben den umfangreichen Fragebogen beantwortet. Der Anteil der Studienempfänger aus dem DACH-Raum lag bei 32% der Studienempfänger. Im gleichen Zeitraum war die Umfrage ebenfalls öffentlich verfügbar und wurde bei LinkedIn beworben [10]. Rund 12% aller Antworten konnten über diesen Kanal gesammelt werden. Von den Befragten gaben 90% an, ein Security Awareness Spezialist zu sein.



Source: LUCY Cybersecurity Awareness Survey 2020

FUSSNOTEN & QUELLEN

01

https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing

02

https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-howprotect-against-phishing

03

https://quotes.thefamouspeople.com/bruce-schneier-939.php

04

ISO27001: https://de.wikipedia.org/wiki/ISO/IEC_27001

05

NIST Cybersecurity Frameworkhttps://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

06

Whitelisting https://en.wikipedia.org/wiki/Whitelisting

07

GDPR https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

08

CCPA – California Consumer Privacy Act -https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

09

Security Awareness Programm: Beispiel SAPF Leitfaden - https://lucysecurity.com/sapf

10

https://www.linkedin.com/feed/update/urn:li:activity:6684493357768552448

KONTAKTE PRO REGION

USA & CANADA

Colin Bastable

colin@lucysecurity.com

AFRICA & MIDDLE EAST

Matthias Ernst

matthias@lucysecurity.com

SOUTH EUROPE & LATAM

Eric Naegels

eric@lucysecurity.com

DACH

Palo Stacho

palo@lucysecurity.com

GLOBAL

Oliver Münchow

oliver@lucysecurity.com

www.lucysecurity.com
www.lucysecurity.com/laws

GLOBAL

LUCY SECURITY AG

Chamerstr. 44
6300 Zug
Switzerland

NORTH AMERICA

LUCY SECURITY USA

13785 Research Blvd
Suite 125
Austin, TX 78750