KALWEIT ITS

Nachhaltige Cybersecurity

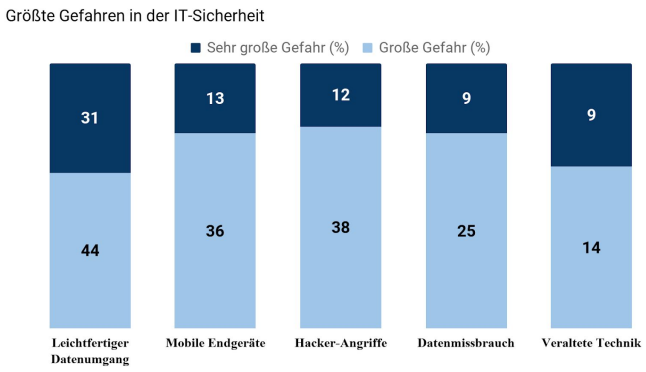
Strategieberatung

INHALT

Einleitung

IT ist heutzutage aus keinem Unternehmen mehr wegzudenken. Tägliche Geschäftsabläufe könnten ohne funktionierende IT nicht bewerkstelligt werden. Aus diesem Anlass entstanden freiwillige wie auch verpflichtende Regularien, konkrete gesetzliche Rahmenbedingungen und damit einhergehend das Bewusstsein für Informationssicherheit. Unternehmen investieren in Sicherheitslösungen, führen regelmäßig Audits durch und versuchen eine Sicherheitskultur einzuführen. Maßnahmen, die der Verantwortung des Unternehmens gegenüber Kunden und Mitarbeitenden gerecht werden sollen, beispielsweise firmeninterne Daten sowie die Daten der Kunden zu schützen. Dennoch scheint sich in der Praxis noch immer der Umstand zu bewahrheiten, dass erfolgreiche Hackerangriffe weiterhin stattfinden.
Statistisch zeigt sich deutlich: "Die Anzahl der täglichen bis wöchentlichen Angriffe hat sich in den letzten fünf Jahren fast verdoppelt."[1]

Unsere These: Wenig nachhaltige Maßnahmen und eine nicht interdisziplinäre Sicherheitsstrategie, die Mensch und Technik integriert, sorgen für den Umstand, dass das Potenzial von Sicherheitsmaßnahmen noch immer nicht effektiv genutzt wird. Zudem gibt es vermehrt Diskrepanzen über die Sicherheitsmaßnahmen, die umgesetzt werden und jene, die tatsächliche Schwachstellen abwehren.



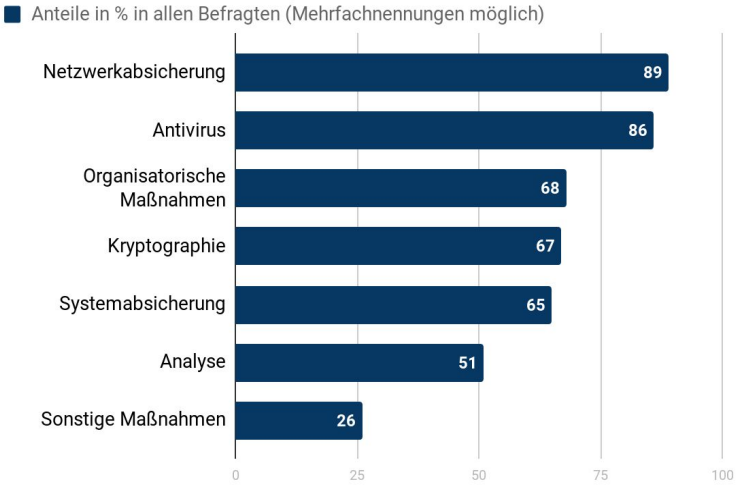
Die aktuelle Lage zeigt, dass die größten Schwachstellen bei dem Faktor Mensch und in der Kommunikation zu finden sind, während der Fokus zur Abwehr eher auf der technischen Seite liegt.

Abbildung: Größte Gefahren gegenüber der IT-Sicherheit.[2]

[1] S. Seite 8 Cyber-Security Report 2017 – Teil 2: Cyber-Risiken in Unternehmen
https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf
[2] s. Seite 14
https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf

“Die größte Gefahr für IT-Sicherheit im Unternehmen geht von einem leichtfertigen Umgang mit Daten seitens der Mitarbeiter aus.”[3]

Genau deshalb ist ein interdisziplinärer Ansatz notwendig, um das Unternehmen und damit verbunden die Schutzziele der IT ganzheitlich und nachhaltig zu schützen.



Die Statistik belegt eindeutig, dass die aktuelle Sicherheitsstrategie der meisten (hier befragten) Unternehmen zu sehr technologisch getrieben ist, eben genau ein ganzheitlicher Ansatz fehlt.

Abbildung: Welche Maßnahmen werden umgesetzt?[4]

[3] s. Seite 14
https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf
[4] s. Seite 16
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6

IT-Security als ganzheitlicher Ansatz

Die oben aufgeführten, repräsentativen Statistiken sowie Erhebungen zeigen deutlich auf, dass die Sicherheitskultur der meisten Organisationen zwar ausgebaut, in jedem Fall durch den fehlenden ganzheitlichen Ansatz aber wenig effektiv ist. Genau deshalb ist notwendig, Cybersecurity für alle Mitglieder einer Organisation verständlich, umsetzbar und selbstverständlich zu machen. Nur so wird die Sicherheitskultur ganzheitlich innerhalb der Organisation zelebriert, nachhaltige Veränderung auf allen Organisationsebenen erst möglich gemacht.

Um das Ziel zu erwirken, Cybersecurity für alle Mitglieder einer Organisation verständlich, umsetzbar und selbstverständlich zu machen, ist es notwendig, Cybersecurity nicht nur in Teilbereichen wie beispielsweise Netzwerksicherheit zu evaluieren. Vielmehr muss die Organisation als ganzheitlicher Sicherheitsfaktor betrachtet werden. Denn Sicherheit ist eine Maßnahme gegen echte Gefahrenquellen, weshalb man alle Faktoren der IT-Sicherheit (Strategie, Organisation, Kultur, Prozess und Technologie) einfließen lassen muss. Ein Angreifer sucht sich zumeist auch nicht einen Teilbereich aus, sondern greift eine Organisation dort an, wo es am verwundbarsten ist.

Ziele der Strategieberatung

Ziel unserer Strategieberatung ist es, diese ganzheitliche Betrachtungsweise der IT-Sicherheit innerhalb der Organisationsstruktur zu integrieren. Wir möchten die Ursachen der IT-Sicherheitsprobleme identifizieren, anstelle nur die Probleme zu beheben. Wir glauben, dass es nur dann möglich ist, wenn man nachhaltig IT-Sicherheit umsetzt. Das wird dadurch möglich, dass wir IT-Sicherheit ganzheitlich evaluieren. Weshalb es notwendig ist, auf interdisziplinäre Ansätze aufzubauen, in dem Wissen, dass Sicherheit immer mit Praxisrelevanz einhergeht. Denn man schützt sich nur vor Dingen, die auch in der realen Praxis eine Gefahr darstellen. Und Praxis, das heißt in der IT immer Technik und Mensch.

Und gerade weil wir Technik und Mensch verstehen, das heißt einen interdisziplinären Ansatz anwenden und das Unternehmen als ganzheitlichen Sicherheitsfaktor evaluieren, ist es uns möglich, nicht nur die Probleme in der IT-Sicherheit, sondern auch deren Ursachen zu lösen.

Prozesse und Technologie agieren dabei unterstützend.

Die Strategieberatung findet unter Einbeziehung der Betroffenen selbst statt,

Schaffung einer Strategie

Es bedarf einer klaren Sicherheitsstrategie, einer Vision und Mission für die IT-Sicherheit. Denn Menschen müssen verstehen, warum Sie tun sollen, was Sie tun sollen. Insbesondere bei einem so heiklen und komplexen Themenfeld wie das der IT-Sicherheit, welches gerne als "Regulierung" verstanden wird. So ist es möglich, auch jeden einzelnen einer Organisation zu mehr Sicherheitsbewusstsein zu motivieren.

Einbindung der gesamten Organisation

IT-Sicherheit ist nicht Chefsache, sondern ein Thema für die gesamte Organisation. Jeder ist für die Sicherheit aller verantwortlich. Die Risiken und Konsequenzen eines Vorfalls und die damit verbundene Verantwortung müssen klar kommuniziert werden. Insbesondere, weil Incidents gerne an die zuständige IT-Abteilung abgegeben werden und dem einzelnen Nutzer die Reichweite seiner Fehlhandlung dadurch nicht bewusst wird. Sicherheit ist eine Verantwortung jedes Einzelnen einer Organisation. Dies gilt es transparent in die Organisation zu kommunizieren, sodass das Sicherheitsbewusstsein alle Bereiche erreicht und innerhalb einer Organisation auch zelebriert wird.

Optimierung der Prozesse

Klare, einfach umsetzbare, wenig regulierende, effektive und praxisnahe Prozessstrukturen, um nicht nur bei Übungen, sondern auch in realen Bedrohungslagen effektiv und gemeinsam Gefahren abwehren zu können.

Zeitgemäßer Einsatz von relevanter Technologie

Zeitgemäße, effiziente und praxisgerechte Umsetzung von Sicherheitstechnologien in der Praxis.

Integration in die Unternehmenskultur

Sicherheit ist keine Hürde oder Regulierung, sondern eine Chance für die Digitalisierung: Gerade weil es Sicherheiten gibt, ist es möglich, mehr machen zu können.
Flugzeuge oder Autos stellen gute Paradebeispiele da: Gerade aufgrund von Sicherheiten können diese Technologien genutzt werden.

Dieses Framing gilt es auch in der Unternehmenskultur zu manifestieren. Wie Dr. Hasib in seinem Buch "Impact of Security Culture on Compliant Behaviour in Healthcare in the USA" belegt, beeinflusst die Kultur sehr stark, ob Mitarbeiter Ihren Beitrag zur Sicherheit der Organisation leisten oder nicht.[5]

[5] vgl. S. 103 "Impact of Security Culture on Compliant Behaviour in Healthcare in the USA", Dr. Mansur Hasib, 2013

Ansatz zur Umsetzung der Strategie

IT-Sicherheit stellt ein effektives Mittel dar, die Schutzziele der IT zu gewährleisten. Diametral zur IT-Security stehen die Usability, die Wirtschaftlichkeit sowie der Datenschutz. Eine ganzheitliche Betrachtungsweise ermöglicht es, IT-Security zur Gewährleistung der Schutzziele der IT angemessen einzusetzen.

Nach unserem Erfahrungswert zeigt sich, dass bei ganzheitlicher Betrachtungsweise des Themenfeldes IT-Security folgender, direkter Mehrwert generiert wird:

- Investitionen in IT-Security amortisieren sich, da Sicherheit ganzheitlich betrachtet wird und die Organisation effizienter und nachhaltiger vor möglichen Risiken geschützt wird
- Es wird eine Praxisnähe hergestellt d.h. IT-Security in der Organisation positiv zelebriert, die Motivation entsteht, sich damit aktiv zu befassen und auszutauschen
- Sicherheit wird nicht mehr als Regulierung verstanden, sondern als Chance mehr machen zu können
- IT-Security wird agiler, bereichs- und funktionsübergreifend
- Maßnahmen in IT-Security erfahren einen langfristigen Nutzen und werden dadurch nachhaltig

Der Prozess zur Umsetzung auf einen Blick

Der Prozess der ganzheitlichen Betrachtung von IT-Security lässt sich im Rahmen eines Projektauftrags realisieren.

Zunächst gilt es im Rahmen der ersten Projektphase "Ordnung schaffen", den aktuellen IST-Zustand der Sicherheitslage einer Organisation kompromisslos zu bestimmen. Innerhalb der zweiten Projektphase "Prozessoptimierung" erfolgt die Entwicklung eines Sicherheitskonzeptes, mit deren Umsetzung eine Prozessoptimierung der IT-Security innerhalb der Organisation stattfindet.
Basierend auf diesem Konzept erfolgt in der dritten Phase "Nachhaltigkeit etablieren" die Entwicklung und Umsetzung von Maßnahmen zur Einhaltung eines kontinuierlichen Schutzstandards durch interne Ressourcen.

Als letzten Schritt gilt es, diese internen Verfahren zu etablieren, die den aktuellen Schutzstandard nicht nur halten, sondern auch selbstständig durch interne Ressourcen in Revision setzen. Dadurch lässt sich ein Kreislauf generieren, der nicht nur ein Sicherheitsniveau gewährleistet und zyklisch in Revision setzt, sondern auch externe Revisionen und damit einhergehende Kosten deutlich minimiert.

Ordnung schaffen

Ziel dieser Phase ist es, zu prüfen, ob der aktuell gültige Schutzstandard innerhalb der Organisation tatsächlich in der Praxis standhält und ob der von der Organisation definierte Schutzbedarf auch in der Praxis von Relevanz zeugt. Durch einen umfangreichen Penetrationstest wird kompromisslos der IST-Zustand des informationstechnischen Systems im Kontext des Sicherheitsniveaus wiedergeben, die aufgezeichneten Protokolle geprüft, ob bisher prozessierte Hackerangriffe überhaupt erkannt, richtig bewertet und entsprechende Gegenmaßnahmen angemessen umgesetzt worden sind. Die gefundenen Schwachstellen werden anschließend durch die jeweiligen Fachabteilungen gefixt.

Die Erkenntnisse dieser Projektphase werden zum Anlass genommen, unklare, nicht praxisnahe oder ineffektive Vorgaben zu identifizieren. Auf Basis dieser Ergebnisse wird die Anforderung der Projekttätigkeit genauer definiert.

Prozessoptimierung

In dieser Projektphase werden die gefunden Sicherheitslücken geschlossen sowie die ineffizienten Vorgaben, Standards, Sicherheitspolicies und Vorgehensweisen durch optimierte und klare Strukturen ersetzt. Nachfolgend wird ein Praxiskonzept konkretisiert, dass auf den alten Standards der Organisation anknüpft, diese regeneriert, konkreter und einfacher formuliert, eine Praxisnähe schafft und insbesondere für alle Mitglieder einer Organisation verständlich, umsetzbar und selbstverständlich macht. Nach dem Schritt der Prozessverbesserung wird die Umsetzbarkeit in die Organisation und damit verbunden in die Organisationskultur gewährleistet.

Hier inkludieren wir interpersonelle Einflüsse, den aktuellen IST-Zustand des Systems, weitere informationstechnische Einflüsse, identifizierte Prozessprobleme sowie unternehmensspezifische sowie anderweitig regulatorische Vorgaben.

Interpersonelle Einflüsse:

selektive Wahrnehmung	Vorurteile/ Wahrnehmung	Recency-Effekt	First-Impression-Effekt	Ziel, Vision des Unternehmens / der IT-Security
Halo-Effekt	Kontakteffekt	Nicolaus-Effekt	Andorra-Effekt	Hierarchie-Problematiken

IST-Zustandsanalyse:

Identifizierte Schwachstellen	Bekannte, nicht gefixte Schwachstellen	Unzureichend gefixte Schwachstellen
Nicht zeitgemäßer Einsatz von Technologien	Nicht identifizierte Sicherheitsvorfälle	Falsch bewertete Sicherheitsvorfälle

Informationstechnische Einflüsse

Fehlende Systemintegration	Integrität der Sicherheitsmaßnahmen	Angemessene Patchkonzepte
Zeitgemäßer Einsatz	Verhältnismäßigkeit	Outsourcing der IT-Infrastruktur

Prozessprobleme

unzureichende Prozessstandards	Hierarchien	Outsourcing der Mitarbeitenden
Praxistauglichkeit	Mitarbeiterausfall	Deadline-Politik

Vorgaben

Regulierungen	Unternehmensstandards
Policies	Anweisungen

Nachhaltigkeit etablieren

In der finalen Projektphase gilt es, das neue Sicherheitskonzept langfristig zu etablieren, den neuen Sicherheitsstandard durch interne sowie externe, zyklisch durchgeführte Auditierungsverfahren auf Beständigkeit zu prüfen. Außerdem gilt es systematische Fehleranalyse durch interne Ressourcen zu etablieren. Weitere Maßnahmen zur Gewährleistung der Nachhaltigkeit ermöglichen es der Organisation, den bereits umgesetzten Sicherheitsstandard langfristig zu halten.

Ergänzende Bausteine dieser Projektphase stellen nachfolgende Themenbereiche dar:

-> mit Meilensteinen steuern, um kompromisslos auch in Problemsituationen den Fokus beizubehalten

-> Prozesse standardisieren, um einen durchgängigen und einheitlichen Sicherheitsstandard zu gewährleisten

-> effiziente Teamnutzung, sodass alle einer Organisation ein angemessenen Basiswissen über IT-Security verfügen

-> minimierte Totzeiten von IT und Mensch, da bei ganzheitlicher Betrachtung die Interaktion zwischen IT und Mensch “Hand in Hand” geht.

-> Selektion, Priorisierung sowie Anpassung der bereits bestehenden, neuen Sicherheitskonzepte, um Sicherheit angemessen neben Usability, Wirtschaftlichkeit und Datenschutz anzuwenden

Über den Autor

Philipp Kalweit - Chief Executive Officer

Philipp Kalweit (Jahrgang 2000) ist Deutschlands begehrtester Hacker und renommierter IT-Sicherheitsexperte. Seit seinem 16. Lebensjahr berät er Unternehmen zu Themen der IT-Sicherheit. Seine Schwerpunkte liegen in der Öffentlichkeitsarbeit sowie Aufklärung, ganzheitlichen Sicherheitsüberprüfungen sowie interdisziplinärer Beratung. 2017 gründete Philipp das Beratungsunternehmen Kalweit ITS GmbH. Zwischen 2017 und 2019 leitete er im Rahmen seiner Unternehmung ein Team im Alter zwischen 21 und 48 Jahren. Heute greift er auf ein weltweites Netzwerk aus freien Mitarbeitern, Expertenteams und Kooperationspartner zurück und beschränkt sich damit nicht nur auf das interne Know How des Unternehmens.

Seine Mission: Nachhaltige Cybersecurity für eine digitale Welt von morgen. Für sein Wirken wurde er von der ZEIT Hamburg am 31.01.2019 als Hamburger des Monats geehrt und von Forbes im gleichen Jahr als einer der bedeutendsten Jungunternehmer der „30 unter 30“ Liste ausgezeichnet.

Philipp ist es wichtig, die Relevanz von IT-Sicherheit gesamtgesellschaftlich zu vermitteln. Durch Keynotes, Präsenz in der deutschen Medienlandschaft oder Kampagnen mit internationalen Unternehmen wie Microsoft, versucht er den Stereotyp "Hacker" aufzubrechen. IT-Sicherheit sollte nach seiner Auffassung umfassend, transparent und für jeden zugänglich sein.

In seiner Freizeit ist Philipp mit seinem Kajak auf der Außenalster unterwegs oder versucht sich im Bouldern und Slacklining.

Über Kalweit ITS

Wir wollen Cybersecurity für alle verständlich, umsetzbar und selbstverständlich machen. Denn Cybersicherheit ist keine Regulierung, sondern eine Chance für die Digitalisierung.

Ein dezentrales Team, dass Unternehmen als ganzheitlichen Sicherheitsfaktor versteht. Ein Team, dass Sicherheit als soziales Thema versteht und deshalb auch Sozialwissenschaften und Philosophie einsetzt.
Denn wir wissen, dass jedes Sicherheitskonzept und jede Sicherheitslösung nur dann wirksam ist, wenn diese auch von den Anwendern akzeptiert wird.

Kalweit ITS - Penetrationstests. Sicherheitsmanagement. Risikomanagement. Consulting. Das sind wir.

Weiterführende Literatur

Wer ist über Security informiert?
https://de.statista.com/statistik/daten/studie/235843/umfrage/informationslage-ueber-cyber-kriminalitaet-in-deutschland/

https://de.statista.com/statistik/daten/studie/863266/umfrage/folgekosten-von-datenlecks-im-gesundheitswesen/

Anzahl Datenlecks
https://de.statista.com/statistik/daten/studie/865084/umfrage/anzahl-datenlecks-und-geklauter-datensaetze-in-den-usa/

Cyber Readiness Report - Deutschland als Anfänger
https://www.hiscox.de/hiscox-cyber-readiness-report/

Welche Maßnahmen werden ergriffen?
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6

Anzahl Cyberangriffe
https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf

Trend Breaches
https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

Pentesting statistics
https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019/

Measure secure culture
http://www.pacis-net.org/file/2012/PACIS2012-005.pdf

Kultur und Verhalten
https://books.google.de/books?id=1f_9AAAAQBAJ&pg=PA95&lpg=PA95&dq=statistics+security+culture&source=bl&ots=ZYA6dqRRqx&sig=ACfU3U2-2vEVvl-pGQO_ZRZMFSkrLw4C0w&hl=de&sa=X&ved=2ahUKEwiRz-imo6fhAhXLjqQKHU9kCNAQ6AEwCXoECAgQAQ#v=onepage&q=statistics%20security%20culture&f=false