NIS2

FÜR FÜHRUNGSKRÄFTE

DIE NEUEN EUROPÄISCHEN COMPLIANCE-ANFORDERUNGEN EINFACH UND VERSTÄNDLICH ERKLÄRT

CHECK POINT™

Marco Eggerling, LL.M,

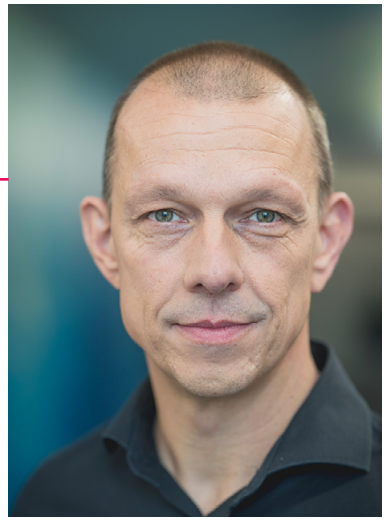
Global CISO,
Check Point Software

„Die NIS2 Direktive wird die Wahrnehmung von regulatorischer Compliance in den europäischen Mitgliedsstaaten nachhaltig positiv beeinflussen und die Notwendigkeit für robuste Sicherheitsprogramme in den Fokus der Geschäftsführung rücken. Auch wird die Zusammenarbeit zwischen der Rechtsabteilung und der Informationssicherheit gestärkt und die Rolle des CISO deutlich von jener des DPO separiert. Das Ziel von NIS2 ist es u.a. den Reifegrad der Informationssicherheit aller involvierter Unternehmen zu steigern, somit ist es auch die Aufgabe des CISO mehr in die Rolle des Beraters der Geschäftsführung zu wachsen."

Peter Sandkuijl,

VP EMEA Engineering,
Check Point Software

„Die NIS2 ist eine Richtlinie, die weder eine Checkliste noch eine Reihe von Mindestanforderungen enthält. Sie beschreibt einen angemessenen Schutz, der natürlich offen für Interpretationen ist. Als Mindestanforderung können wir jedoch davon ausgehen, dass Firewall- und Intrusion-Prevention-Technologien im Netzwerk, ein ausreichender Schutz der Endgeräte, die Implementierung von Mehrfaktor-Authentifizierung, Datenverschlüsselung und Zugangsbeschränkung sowie andere bewährte Verfahren dazugehören."



NIS2
Eine Richtlinie mit Spielraum

Am 14. Dezember 2022 wurde eine neue Cybersicherheitsrichtlinie – Netzwerk- und Informationssicherheits Richtlinie 2 (NIS2) – vom Parlament und dem Rat der Europäischen Union verabschiedet. In Reaktion auf die seit Jahren zunehmende Cyberbedrohungslage soll die neue Richtlinie – Nachfolger des 2016 verabschiedeten NIS1 – die Cybersicherheitsmaßnahmen von Unternehmen und Einrichtungen mit Systemrelevanz erhöhen und vereinheitlichen und so die Cyberrisikolage der europäischen Wirtschaftslandschaft minimieren.

Mehr als 160.000 Unternehmen und Einrichtungen aus 27 EU-Mitgliedsstaaten müssen, bis zum 17. Oktober 2024, Maßnahmen zur Einhaltung der NIS2-Richtlinie ergreifen, die Mitgliedsstaaten ihre Vorgaben in nationales Recht überführen und konkretisieren. In Deutschland liegt ein erster Entwurf für ein NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) bereits vor. Hierbei handelt es sich um ein Änderungsgesetz, das unter anderem das BSI-Gesetz verändern wird. Daneben wird das KRITIS-Dachgesetz ab 2024 die EU RCE umsetzen, auch hier liegt bereits ein Entwurf vor. Beide Initiativen sollen die Resilienz für KRITIS erhöhen.

Am 18. Oktober 2024 soll das NIS2UmsuCG in Kraft treten. Vier Jahre, bis Ende 2028, haben betroffene Unternehmen dann Zeit, die neuen Vorgaben zu implementieren und das erste Audit vorzulegen. Davor schon werden die neuen Verordnungen aber greifen. Kommt es zu einem erfolgreichen Cyberangriff, müssen die in NIS2 vorgesehenen Berichte umgesetzt werden.

Die von Parlament und Rat der Europäischen Union verabschiedeten Vorgaben bleiben unspezifisch. Ein konkretes Set an Minimalvorgaben sucht man im NIS2-Gesetzestext vergebens. Sie sind erst im Oktober, mit der Umsetzung durch die beauftragten nationalen Stellen, zu erwarten.

Der Versuch, sich ein umfassendes Bild von den Vorgaben zu machen und alle erforderlichen Maßnahmen einzuleiten, wird so wesentlich erschwert. Schon Informationssicherheitsexperten stoßen hier an ihre Grenzen. Noch mehr jedoch leiden die Führungskräfte von Einrichtungen und Unternehmen unter der unklaren Ausgangslage, betrifft sie doch die IT- und die Cyberwelt. Und das ist ein echtes Problem. Denn mit NIS2 werden sie erstmals persönlich für Misserfolge ihrer Cybersicherheit zur Verantwortung gezogen werden.

Die erste Cybersicherheitsrichtlinie, die auch Führungskräfte in Haftung nimmt

Unternehmensstrafen für IT-Sicherheitsverstöße gibt es in Europa bereits seit der Einführung der DSGVO 2015. Seitdem wurden sie immer weiter verschärft, so dass bei schweren Verstößen mit bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes gerechnet werden muss. NIS2 geht einen Schritt weiter. Zusätzlich werden – bei einem nachgewiesenen Fehlverhalten – die Führungskräfte eines Unternehmens, in NIS2 als „Leitungsorgane" bezeichnet, in Haftung genommen.

NIS2 sieht vor, dass die Geschäftsführung die Risikomanagement-Maßnahmen für Cybersicherheit billigt und die Umsetzung in ihrer Einrichtung oder ihrem Unternehmen überwacht. Sie muss sicherstellen, dass im Fall eines erfolgreichen Angriffs betroffenen Partnern, Zulieferern und Kunden sowie den zuständigen nationalen Behörden Meldung gemacht wird.

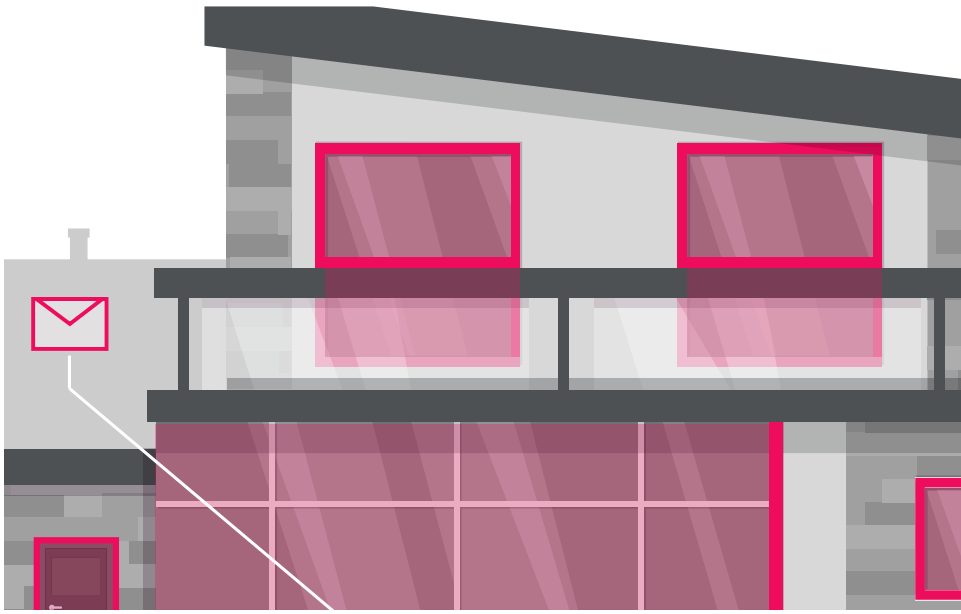
Um diesen Aufgaben gerecht zu werden, soll sie regelmäßig an Cybersicherheitsschulungen teilnehmen, die sie in die Lage versetzt, Cyberrisiken und Cybersicherheitsmaßnahmen zu erkennen und zu bewerten. Kommt sie dem nachgewiesenermaßen nicht nach, kann sie – persönlich – für die Vernachlässigung ihrer Sorgfaltspflicht haftbar gemacht werden.

Wie hoch die Strafe dann ausfällt, wie sie konkret auszusehen hat, kann jeder EU-Mitgliedsstaat für sich entscheiden. Doch gibt NIS2 vor, dass die Strafe *„wirksam, verhältnismäßig und abschreckend"* zu sein hat. Explizit erwähnt wird, dass die Geschäftsführung von der Wahrnehmung ihrer Leitungsaufgaben entbunden werden kann, bis die NIS2-Mängel ihrer Einrichtung beseitigt sind.

NIS2 für Führungskräfte

Aus diesem Grund ist es absolut erforderlich, dass auch die Geschäftsführung – und damit auch Nicht-Informationssicherheitsexperten – sich mit NIS2 vertraut macht, grundlegend versteht, um was es geht und begreift, wie weit die neuen Vorgaben reichen. Schließlich ist sie es, die ab Oktober dieses Jahres bei einem nachgewiesenen Fehlverhalten zur Verantwortung gezogen werden wird.

Die NIS2 wird also umfassende Änderungen für die betroffenen Unternehmen bringen. Vielfach stellt sich jedoch die Frage, wie eine Umsetzung gelingt, um die IT-Sicherheit zu erhöhen und die Anforderungen nicht nur aus Compliance-Sicht abzuhaken. Die folgende Schritt-für-Schritt Anleitung soll anhand eines Hauses Aufschluss darüber geben, wie sich Daten und IT-Infrastruktur im Sinne der NIS2 absichern lassen. Letztlich gilt es für Führungskräfte einen Sicherheitsvorfall zu verhindern. Dies lässt sich mit physischen Sicherheitsmaßnahmen zur Abwehr von Einbrechern vergleichen.



Um das Risiko eines erfolgreichen Einbruchs zu reduzieren (und die Kosten der Hausratversicherung zu senken), müssen Grundstück und Gebäude in ausreichendem Maße und nachweislich vor dem Zutritt unberechtigter Dritter geschützt sowie Grundstücksgrenzen abgesichert werden.

Ebenso verhält es sich mit der IT-Infrastruktur und den Daten von Einrichtungen und Unternehmen, die von NIS2 betroffen sind. Auch diese müssen, um das Risiko eines erfolgreichen Cyberangriffs zu reduzieren, geschützt werden. Deshalb wird im folgenden die Absicherung des Hauses als Metapher für die Absicherung der IT-Infrastruktur genutzt. Um die NIS2-Vorgaben voll zu erfüllen, muss dieser Schutz umfassend, effektiv, kontinuierlich und nachweisbar sein. Für welche Cybersicherheitsbereiche NIS2-Konformität nachgewiesen werden muss, darüber gibt im NIS2-Rechtstext das Kapitel IV Auskunft.

Kapitel IV, Artikel 21, Absatz 2 – der Sicherheitsbereichskatalog, auf den es ankommt

Insgesamt setzt sich der NIS2-Rechtstext aus 10 Kapiteln mit 46 Artikeln und 3 Anhängen zusammen. Die meisten dieser Kapitel betreffen Verpflichtungen der europäischen Mitgliedsstaaten. Anders Kapitel IV. Hier werden in Artikel 21 die von betroffenen Unternehmen und Einrichtungen auf ihre NIS2-Konformität zu überprüfenden Bereiche dargelegt.

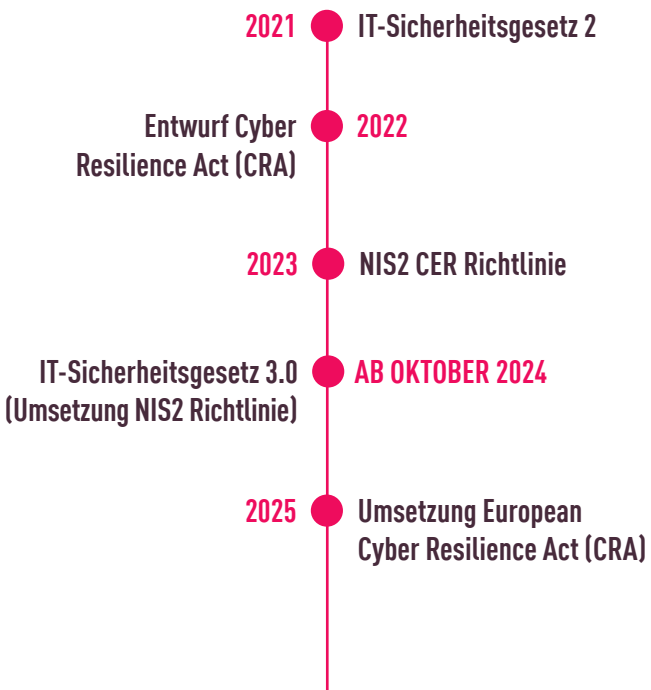
Konkrete Maßnahmen werden dabei nicht genannt. In der Vorgabe heißt es lediglich: Unternehmen müssen *„geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, die dem Stand der Technik und den geltenden Normen entsprechen*".

Die Bereiche, auf die diese Vorgabe Anwendung finden soll, umfassen:

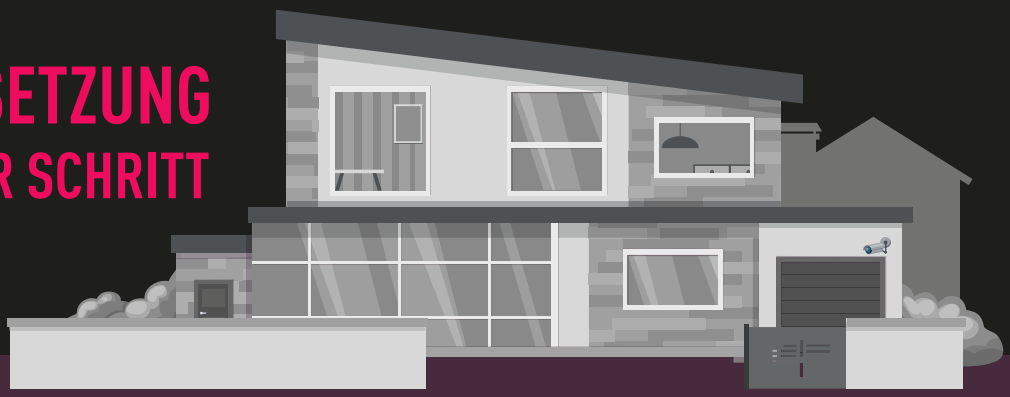
1. Konzepte für die Risikoanalyse und Sicherheit,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs,
4. Sicherheit der Lieferkette,
5. Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen,
6. Bewertung der Wirksamkeit von Maßnahmen,
7. grundlegende Cyberhygieneverfahren und Cybersicherheitsschulungen,
8. Konzepte und Verfahren für Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Zugriffskontrolle und Asset Management und
10. Authentifizierung und Kommunikation.

Informationssicherheitsexperten genügen diese Angaben, um zu verstehen, welche IT-Sicherheitsbereiche betroffen sind und welche Maßnahmen an den entsprechenden Stellen mit hoher Wahrscheinlichkeit zu implementieren sind. Nicht-Informationssicherheitsexperten werden mit den Vorgaben jedoch nur wenig anzufangen wissen.

Visualisieren wir diese Vorgaben deshalb nun einmal im Kontext eines Objektschutzes für ein Haus samt Grundstück und gehen die einzelnen Vorgaben dann Schritt für Schritt durch. Dieser Ansatz wurde gewählt, um zu verdeutlichen, dass eine nachträgliche Erkennung von Sicherheitsvorfällen wenig zielführend ist. Die Kosten für einen solchen liegen nach dem Cost of a Data Breach Report von IBM im Durchschnitt bei über vier Millionen Euro. Obwohl die Strafverfolgungsorgane in den vergangenen Jahren einige Erfolge wie bei Emotet und Anderen vermelden konnten, bleibt die Erfolgsrate gering. Deshalb empfiehlt sich nicht nur beim Thema Cybersicherheit ein präventiver Ansatz zur Verhinderung eines Einbruchs in die IT-Systeme wie auch in das Haus selbst:



NIS2-UMSETZUNG
SCHRITT FÜR SCHRITT



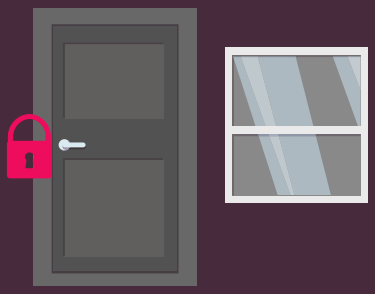
OBJEKTÜBERWACHUNG
Konzepte für die Risiko-analyse und Sicherheit.

WACHMANN
Bewältigung von Sicherheitsvorfällen.

HAUSRATVERSICHERUNG
Aufrechterhaltung des Betriebs.

ZUFAHRTSWEGE
Sicherheit der Lieferkette.

HAUSTÜR, FENSTER, BRIEFKASTEN & HAUSSPRECHANLAGE
Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, Authentifizierung und Kommunikation.

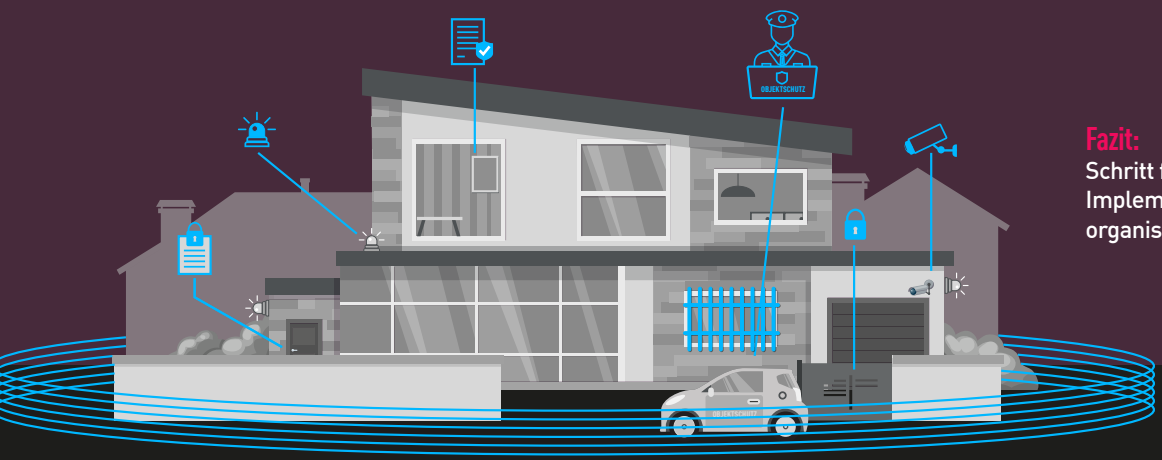


ALARMANLAGE & VIDEOÜBERWACHUNG
Bewertung der Wirksamkeit von Maßnahmen.

BEWOHNERSCHULUNG
Grundlegende Cyber-hygieneverfahren und Cybersicherheitsschulungen.

SCHLÖSSER
Konzepte und Verfahren für Kryptografie und Verschlüsselung.

BEWOHNER, BESUCHER- UND HAUSRATSLISTE
Sicherheit des Personals, Zugriffskontrolle und Asset Management.



Fazit:
Schritt für Schritt-Anleitung für die Implementierung der technischen und organisatorischen Maßnahmen für NIS2.

1. OBJEKT-ÜBERWACHUNG

Konzepte für die Risiko-analyse und Sicherheit

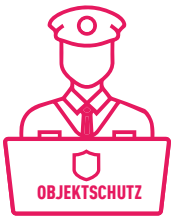
Um Ihr Haus und Grundstück vollständig abzusichern, müssen Sie es zunächst einmal umfassend in den Blick nehmen. Sie müssen sämtliche Assets und Infrastrukturen, sämtliche Sicherungsmaßnahmen, Sicherheitslücken und -risiken absichern.. Hierzu bestellen Sie Sicherheitsexperten, die eine professionelle Bestandsaufnahme vornehmen, darauf basierend Risiken einschätzen und dann eine Analyse vorlegen auf deren Basis dann eine umfassende Sicherheitsplanung, die alle Bereiche Ihres Hauses, Ihres Gartens, Ihres gesamten Grundstücks, abdeckt.

Ebenso verhält es sich, wenn Sie Ihre Daten umfassend absichern wollen. Auch hier kommen Sie an einer umfassenden Bestandsaufnahme Ihrer IT-Infrastruktur, einer Definition und Analyse sämtlicher Risiken nicht herum, wollen Sie eine effektive Planung zur Implementierung einer NIS2-konformen Sicherheitslandschaft vornehmen.

To-do: Beauftragen Sie Beratungsspezialisten mit einer Gap- sowie einer Risikoanalyse Ihrer gesamten IT-Landschaft auf Basis von ISO 27001. Nutzen Sie die so gewonnenen Daten dann als Basis für eine NIS2-konforme Sicherheitsplanung Ihrer gesamten IT-Infrastruktur und Datenlandschaft.

2. WACHMANN

Bewältigung von Sicherheitsvorfällen



Als nächstes muss eine Wachmannschaft angestellt werden. Diese muss das abzusichernde Objekt regelmäßig besichtigen, und im Fall eines Vorfalls Maßnahmen ergreifen, um sie abzustellen. Finden sich Hinweise auf einen Sicherheitsvorfall, muss dieser untersucht, muss das Objekt auf mögliche Schäden überprüft, müssen Maßnahmen zur Abstellung des Sicherheitsvorfalls eingeleitet werden.

Dasselbe Prinzip gilt auch für eine IT-Infrastruktur. Statt einem Wachmann operieren hier Informationssicherheitsexperten. Deren Handlungen im Fall einer Krise müssen schon im Vorfeld geplant und vorbereitet werden. Entdeckte Vorfälle müssen analysiert und ausgewertet, geeignete Sicherungsmaßnahmen getroffen werden. Ein Bericht muss erstellt und an betroffene Partner, Zulieferer und Kunden sowie an die verantwortliche zentrale Dienstelle des jeweiligen Staates gesandt werden.

To-do: Beauftragen Sie Informationssicherheitsexperten mit Penetrationstests. Lassen Sie Ihre Incident Response-Bereitschaft bewerten. Außerdem sollte ein dokumentiertes Verfahren für Zwischen- oder Ausfälle vorhanden sein, das für die Prüfungsstandards gilt. Im Zweifel empfiehlt sich das Engagement von Dienstleistern, um die Aufgaben als Managed Service einzukaufen anstelle ein eigenes Security Operation Center (SOC) aufzubauen.

Managed Security Services (IDC): Cybersicherheit ist nicht länger nur das Spielfeld von CIOs oder CISOs. Der Vorstand und der Rest der Geschäftsleitung müssen in der Lage sein, darauf zu vertrauen, dass ihre Cybersicherheitsstruktur gegen die Arten von Cyberangriffen, die gegen sie gerichtet sind, resilient genug ist. Die alte Strategie, mehr technische Tools und mehr Geld für den Schutz des Unternehmens auszugeben, sind nutzlos, wenn die geschulten Fachkräfte, die die unzähligen Tools konfigurieren, abstimmen und überwachen, nicht vorhanden oder unbezahlbar sind. Anbieter von Managed Security Services springen in die Lücke, indem sie eine bessere Sicherheit zu einem niedrigeren Preis zu ermöglichen.

3. HAUSRAT-VERSICHERUNG

Aufrechterhaltung des Betriebs: Backup, Disaster Recovery, Business Continuity Management

Für den Fall, dass doch einmal ein Einbruch gelingt, muss vorgesorgt werden. Bewohner sollten nur so kurz wie möglich vom Einbruch, vom Diebstahl ihrer Güter, betroffen sein. Im Fall eines Hauses wird dies über den Abschluss einer Hausratversicherung bewerkstelligt.

Auch die IT-Infrastruktur muss, im Fall eines erfolgreichen Angriffs, möglichst schnell wiederhergestellt sein. Dies erfolgt über Backup Management, Disaster Recovery- und Krisenmanagement.

To-do: Beauftragen Sie Informationssicherheitsexperten mit einer Prüfung und Analyse ihrer Bereitschaft im Krisenfall. Rüsten Sie Ihre IT-Landschaft für den Fall eines erfolgreichen Angriffs zusätzlich auf. Minimieren Sie den Schaden durch die Umsetzung einer Zero Trust Architektur.

4. ZUFAHRTSWEGE

Sicherheit der Lieferkette

Ihr Haus wird beliefert. Waren werden abgeholt. Externe erbringen Dienstleistungen auf Ihrem Grundstück. Damit es hierbei nicht zu einem Sicherheitsvorfall kommt, sollten Sie Ihre Lieferanten und Dienstleister vorsichtig auswählen. Auch eingekaufte Produkte sollten vorher überprüft werden, damit Sie sich kein Trojanisches Pferd ins Haus stellen.

Mit NIS2 müssen Unternehmen nun auch ihre Supply Chains – sowohl die physischen als auch die digitalen – umfassend vor potenziellen Angreifern absichern. Das bedeutet, dass sämtliche Lieferketten, die in das Unternehmen oder die Einrichtung hinein und aus ihm hinausgehen, auf mögliche Schwachstellen untersucht, die entsprechenden Bereiche zusätzlich abgesichert werden müssen.

To-do: Beauftragen Sie Informationssicherheitsexperten mit der Bestandsaufnahme und Analyse sämtlicher Supply Chains, die Ihre Einrichtung betreffen. Verschaffen Sie sich einen Überblick über sämtliche Risiken und lassen Sie sie zusätzliche Maßnahmen implementieren, um diese zu minimieren.

5. & 10. HAUSTÜR, FENSTER, BRIEFKASTEN, TELFONE, UND HAUSSPRECHANLAGE

Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen & Authentifizierung und Kommunikation: Firewalls, Netzwerksicherheit

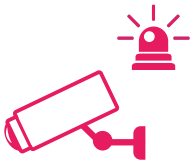
Um Ihr Haus vor Einbrechern zu schützen, gilt es die Haustür und den Briefkasten mit einem sicheren Schloss und stabilen Schlüsseln sowie Fenster mit Sicherheitsglas in der gewünschten Stärke auszustatten. Darüber hinaus müssen Sie auch die Kommunikation innerhalb des Hauses sowie zwischen Haus und Außenwelt effektiv absichern. Außenstehende sollen sich nicht unerlaubt Zugang zu oder gar Zugriff auf die Kommunikation verschaffen können.

Dasselbe gilt für den Zugriff auf die Daten Ihrer IT-Infrastruktur. Zugänge und Zugriffe müssen über moderne Authentifizierungsverfahren abgesichert werden. Außerdem muss sichergestellt sein, dass Außenstehende sich nicht unerlaubt Zugriff auf die Kommunikation verschaffen, Daten ergänzen oder abschöpfen können. Hierzu muss die Text-, Audio- und Video-Kommunikation, müssen die Notfallkommunikationssysteme vor Fremdzugriffen abgesichert werden.

To-do: Segmentieren Sie die Netzwerke in unterschiedliche Bereiche mit verschiedenen Sicherheitsstufen. Setzen Sie Next Generation Firewalls ein, um den Zugriff auf Ihren Server zu kontrollieren und nur berechtigten Verkehr durchzulassen. Implementieren Sie Intrusion Prevention Systems (IPS) zum Erkennen und Verhindern von unerwünschtem Eindringen und einen rollenbasierten Zugang nach dem Least-Privilege-Prinzip. Stellen Sie außerdem sicher, dass alle APIs, die von Ihrem Server verwendet werden, authentifiziert, autorisiert und verschlüsselt sind, um Datenlecks zu vermeiden. Richten Sie zudem ein modernes Identity und Access Management (IAM)-System ein. Lassen Sie sie eine Multifaktor-Authentifizierung einrichten und setzen Sie auf Zero Trust, wenn es um Zugriffsrechte geht. Weitere wichtige Technologie-Konzepte wie SASE, CNAPP und XDR sollten ebenfalls umgesetzt werden.

6. ALARMANLAGE UND VIDEOÜBER-WACHUNG

Bewertung der Wirksamkeit von Maßnahmen: Sicherheit in Netzwerken und Informa-tionssystemen



Um nun am und im Haus für Sicherheit zu sorgen, muss eine Alarmanlage installiert werden. Ihre Sensoren, Blinklichter und Alarmmelder stellen sicher, dass verdächtige Bewegungen im Haus schnell wahr-genommen und Gegenmaßnahmen ergriffen werden können.

Ebenso wie das Haus, seine Zimmer und Flure, seine Ein- und Ausgänge mit einer Alarmanlage abgesichert werden müssen, müssen auch die Netzwerke und Informationssysteme der IT-Infrastruktur umfassend ab-gesichert werden. Unterschiedliche Sicherheits-Tools und -Plattformen stehen hierfür zur Verfügung.

To-do: Beauftragen Sie Informationssicherheitsexperten mit der Auswahl, Implementierung und Wartung der für NIS2 erforderlichen Sicherheitssysteme und leiten Sie eine kontinuier-liche Berichterstattung ein. Richten Sie Überwachungssysteme ein, um ungewöhnliche Aktivitäten in Echtzeit zu erkennen und darauf zu reagieren. Eine zentrale Sicherheitsplattform mit Automatisierungsmöglichkeiten wie ML und KI unterstützt bei der Absicherung der Netzwerke und Systeme.

7. BEWOHNER-SCHULUNG

Grundlegende Cyber-hygieneverfahren und Cybersicherheits-schulungen

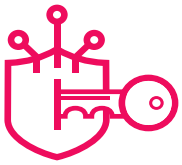
Schließlich müssen auch die Bewohner des Hauses mit der Bedrohungslage des Anwesens vertraut gemacht werden. Sie können vielleicht nicht die einzelnen Sicherheitstools bedienen und sich mit der gesamten Sicherheitslage vertraut machen, sie können aber so geschult werden, dass ihnen verdächtigtes Verhalten auffällt und sie auf grundlegende Fallen, die ihnen Angreifer stellen, nicht hereinfallen.

Dasselbe gilt auch für NIS2. Grundlegende Cyberhygiene-Maßnahmen und Cybersicherheitstrainings zur Anhebung des Sicherheitsbewusstseins helfen, Belegschaften fit für den Ernstfall zu machen und schon im Vorfeld – präventiv – tätig zu werden.

To-do: Beauftragen Sie Schulungsexperten damit, regelmäßige IT-Sicherheitsschulungen und -Trainings für Ihre Informationssicherheitsteams sowie Trainings zur Anhebung des Sicherheitsbewusstseins Ihrer gesamten Belegschaft durchzuführen. Diese Schulungen sollten sowohl regelmäßig erfolgen als auch abwechslungsreich gestaltet und mit entsprechenden Metriken auf Effizienz überprüft werden. Nur so wird es Ihnen gelingen, im Kontext von NIS2 erfolgreich wissensbasierte Entscheidungen zu fällen.

8. SCHLÖSSER

Konzepte und Verfahren für Kryptografie und Verschlüsselung



Um die Zugänge zum Grundstück und Haus, um Ihren Besitz im Haus vor unberechtigtem Zugang und Zugriff zu schützen, bringen Sie unterschiedliche Schlösser an. Ohne passenden Schlüssel kann kein Unberechtigter diese öffnen. Um die Sicherheit zu erhöhen, bewahren Sie die Schlüssel an einem sicheren Ort, fern von den Zugriffsmöglichkeiten eines unberechtigten Dritten auf.

Dasselbe Prinzip gilt auch für Ihre Daten, der Zugang zu ihnen sollte nur auf der Basis von „need to know“ erfolgen. Um sie sicher zu speichern, zu verarbeiten und auszutauschen – ohne, dass unberechtigte Dritte sich unerlaubt Zugang oder Zugriff verschaffen können – müssen diese verschlüsselt werden. Hierbei kommen kryptographische Verfahren zum Einsatz.

To-do: Beauftragen Sie Informationssicherheitsexperten mit der Implementierung der erforderlichen Technologien, Prozeduren und Richtlinien, um sicherzustellen, dass Ihre Daten stets verschlüsselt sind. Denken Sie auch an quantensichere Verschlüsselungsmethoden, um auf die Gefahren von morgen vorbereitet zu sein.

9. BEWOHNER, BESUCHER - UND HAUSRATLISTE

Sicherheit von HR-Prozessen, Zugriffs-kontrollrichtlinien, Asset Management

Um sicherzustellen, dass nur Berechtigte Grundstück und Haus betreten können, dass sämtlicher Hausrat auf dem Grundstück verbleibt, ist es erforderlich, Listen anzufertigen, in denen Bewohner, legitime Besucher und Hausrat verzeichnet sind. Auch diese müssen vom unerlaubten Zugriff durch Dritte geschützt werden. Verwahren Sie die wichtigsten Wertgegenstände und Dokumente in einem Safe.

Dasselbe gilt für Daten aus der Personalabteilung, die Zugriffskontrollrichtlinien und das Asset Management. Auch sie müssen zusätzlich abgesichert werden, bilden sie doch den Grundstock für ein effektives Identity- und Access Management.

To-do: Beauftragen Sie Informationssicherheitsexperten mit der Absicherung der für ein funktionierendes IAM-System erforderlichen Identitätsdaten. Berücksichtigen Sie dabei, dass auch Assets mittlerweile über digitale Identitäten verfügen. Bewahren Sie sensible Daten verschlüsselt und in sicheren, isolierten Speicherbereichen auf, um die Auswirkungen eines möglichen Datenlecks zu minimieren.

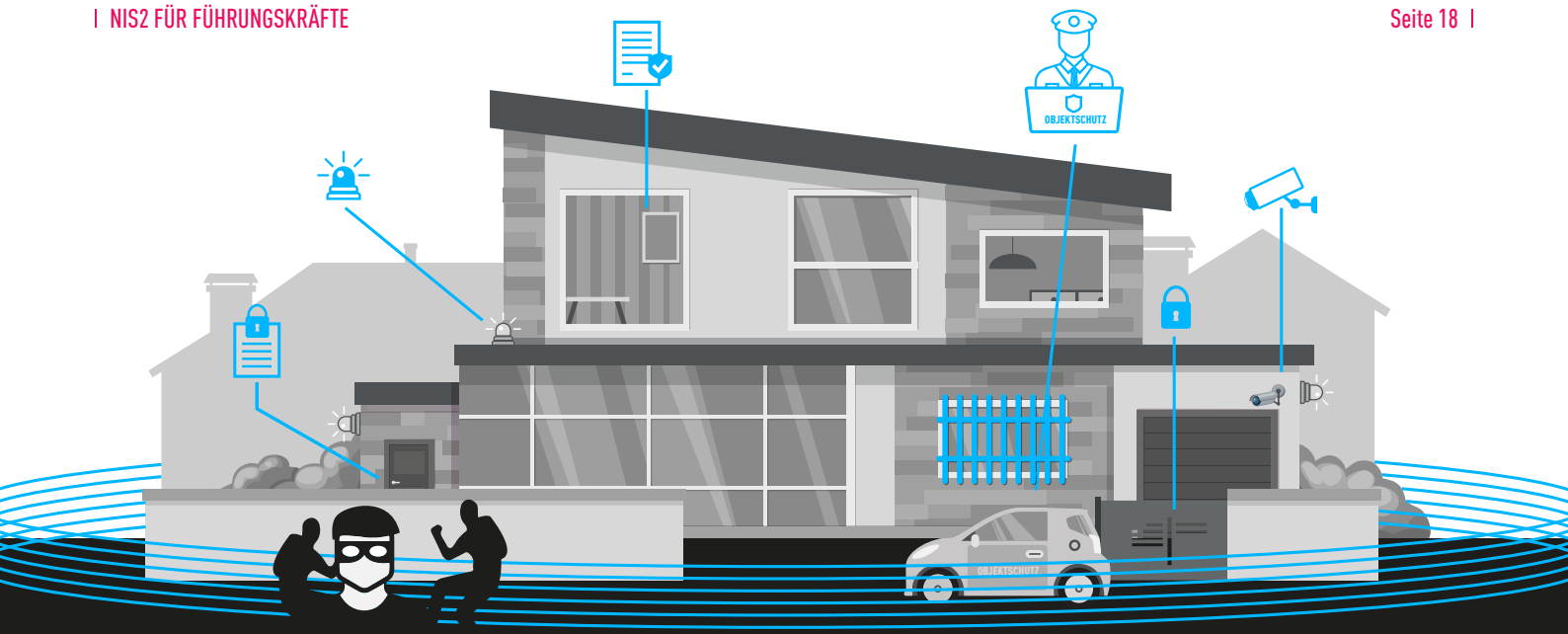
NIS2 – Wie Führungskräfte jetzt vorgehen sollten

Mit der EU-Sicherheitsrichtlinie NIS2 werden Cybersicherheitsmaßnahmen in ganz Europa ein einheitlicher Rahmen gegeben. Bislang orientieren sich Informationssicherheitsexperten vor allem an internationalen Standards wie der NIST, CIS Controls, ISO 27001 und anderen. Cyberrisiken sollen so spürbar reduziert werden. Damit dieser Plan gelingen kann, ist es unabdingbar, dass sich neben den Informationssicherheitskräften auch die Führungskräfte der betroffenen Unternehmen und Einrichtungen in die Implementierung und Aufrechterhaltung der NIS2-Compliance ihrer IT-Systeme aktiv einbringen.

Als Führungskräfte müssen Sie:

1. **Sensibilisierung:** sich grundlegend mit der Materie der Cybersicherheit vertraut machen, so dass Sie in engem Austausch mit ihren Informationssicherheitsexperten stehen, von diesen informiert werden und ihnen fundierte Weisungen erteilen können.
2. **Personal:** sich eine agile Informationssicherheitsabteilung aufbauen, mit dem sich die erhöhten Anforderungen von NIS2 bewerkstelligen lassen. Dabei wird es unerlässlich sein, neben dem Chief Information Security Officer (CISO) für die Datensicherheit auch einen Data Protection Officer (DPO) einzusetzen. Es sollte tunlichst darauf geachtet werden, nicht einer Person beide Posten zu übertragen, sondern die Aufgaben sinnvoll untereinander aufzuteilen.
3. **Audit:** sicherstellen, dass die einzelnen Bereiche einer kritischen Prüfung und Analyse hinsichtlich der Risikolage unterzogen, an NIS2 angepasst und NIS2-konform auditiert werden.
4. **Incident Response:** sicherstellen, dass Vorkehrungen für den Fall eines erfolgreichen Cyberangriffs auf das Unternehmen oder die Einrichtung getroffen werden. Partner, Zulieferer und Kunden, sowie die entsprechenden nationalen Behörden, werden dann schnellstmöglich informiert werden müssen. Die Zeitvorgaben für die Meldung von Vorfällen umfassen eine Frühwarnung, die innerhalb von 24 Stunden nach Kenntniserlangung über den Vorfall an die Behörde erfolgen muss, eine bereits detailliertere und formellere Meldung innerhalb von 72 Stunden und einen Abschlussbericht, einen Monat nach Einreichung der Meldung.

Nur, wenn Geschäftsführung und Informationssicherheitsfachleute an einem Strang ziehen, kann die Umstellung der Cybersicherheit auf NIS2 gelingen. Es handelt sich hier nicht um ein simples Projekt, nicht um eine Aufgabe von wenigen Wochen oder Monaten. NIS2 ist eine kontinuierliche, langfristige Aufgabe. Ab 2028 werden Unternehmen jedes Jahr die NIS2-Konformität ihrer IT-Infrastruktur nachweisen müssen. Sie werden belegen müssen, dass sie *„geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“* ergriffen haben, *„die dem Stand der Technik und den geltenden Normen entsprechen“*.



Sie benötigen Hilfe bei der Umstellung auf NIS2? Kontaktieren Sie unser Expertenteam. Sie überprüfen die bestehenden Sicherheitsmaßnahmen Ihrer IT-Infrastruktur im Hinblick auf deren NIS2-Compliance und unterstützen, um die passenden – NIS2-konformen – organisatorischen wie technischen Lösungen zu finden und umzusetzen.

Werden Sie aktiv und kommen Sie mit uns ins Gespräch: nis2@checkpoint.com

Weitere Ressourcen zum Vertiefen und Nachlesen:

- NIS2 Readiness Assessment
- Check Point Security Consulting
- Infinity Global Services
- Strategische Bereitschaft: Effektive Vorbereitung auf die NIS2-Konformität
- Check Point erläutert was NIS2 für Unternehmen bedeutet

CHECK POINT™