Ministerium des Innern
des Landes Nordrhein-Westfalen

Wirtschaftsspionage

So schützen Sie Ihr Unternehmen

www.im.nrw

Nordrhein-Westfalen ist zu Recht stolz auf seine leistungsfähige und innovative Wirtschaft. In unserem Land gibt es viele umsatzstarke Unternehmen, DAX-Konzerne sowie über 730.000 kleine und mittlere Betriebe. NRW ist zugleich auch Standort von renommierten Universitäten und Fachhochschulen, Forschungseinrichtungen sowie Technologie- und Gründerzentren.

Eine Schattenseite des Erfolgs: Fremde Staaten und konkurrierende Unternehmen interessieren sich für die Daten und das Know-how nordrhein-westfälischer Firmen. Wirtschaftsspionage, die von fremden Staaten gelenkte oder gestützte Spionage gegen Unternehmen, nimmt stetig zu. Nach Schätzungen ist jedes zweite deutsche Unternehmen betroffen.

Der nordrhein-westfälische Verfassungsschutz leistet intensive Präventionsarbeit zur Abwehr von Wirtschaftsspionage, damit die Unternehmen notwendige Schutzmaßnahmen treffen, Hinweise früh erkennen und mögliche Gefahren rechtzeitig abwenden können. Ziel ist ein bestmöglicher Schutz gegen den Verlust wertvoller, zumeist existenzieller Betriebs- und Geschäftsgeheimnisse.

Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes besuchen Unternehmen, Verbände, Universitäten, Forschungseinrichtungen, Behörden oder sonstige Einrichtungen in Nordrhein-Westfalen, um Vorstände, Sicherheitsbeauftragte und Mitarbeiter zu sensibilisieren. Nutzen Sie dieses für Sie kostenfreie Angebot. Der nordrhein-westfälische Verfassungsschutz steht Ihnen jederzeit als kompetenter und vertraulicher Partner zur Seite.

Herbert Reul
Minister des Innern
des Landes Nordrhein-Westfalen

Ihr direkter Draht zum nordrhein-westfälischen Wirtschaftsschutz

E-Mail **wirtschaftsschutz@im1.nrw.de**
Telefon **0211 871 2821**
Website **www.im.nrw/wirtschaftsschutz**

Wirtschaftsspionage - ein Thema für Ihr Unternehmen?

Geschätzt rund 220 Milliarden Euro Schaden entstehen der deutschen Wirtschaft nach aktuellen Studien jährlich durch Spionage, Sabotage und Datendiebstahl. Die Dunkelziffer dürfte noch höher liegen, weil manche Unternehmen aus Sorge vor Imageschäden nicht über mögliche Angriffe und dessen Folgen sprechen.

Unter Wirtschaftsspionage versteht man staatlich gelenkte Spionage. In manchen Ländern der Welt gibt es rechtliche Regelungen, die den Nachrichtendiensten Wirtschaftsspionage erlauben. Mit fremdem Know-how soll die eigene Wirtschaft unterstützt werden.

Im Fokus stehen insbesondere

- das Know-how von Unternehmen sowie sensible Daten zu ihren Produkten, wie beispielsweise Konstruktionspläne, Fotos und Rezepturen,
- Dienstleistungen sowie die dazugehörigen Informationen zu Strategien, Organisation und Logistik,
- Personal-, Kunden- und Lieferantendaten.

Untersuchungen haben gezeigt, dass gerade kleine und mittlere Unternehmen mit ihren innovativen Produkten das Hauptangriffsziel von Wirtschaftsspionen in Deutschland sind. Nahezu alle Branchen sind von Wirtschaftsspionage betroffen. Bei jedem zweiten Unternehmen in Deutschland wurde ein Spionageangriff festgestellt oder es gab zumindest erkennbare Anhaltspunkte für einen entsprechenden Verdacht. Gerade beim Datendiebstahl bemerken Unternehmen häufig gar nicht, dass sie ausspioniert werden. Viele Unternehmen sehen davon ab, staatliche Stellen einzuschalten, weil sie Angst vor negativen Konsequenzen haben oder den Aufwand scheuen. Dies spielt den Angreifern in die Hände.

Ein schneller Informationsaustausch zwischen Unternehmen, Sicherheitsbehörden und der Wissenschaft bietet hingegen die Chance,

- potentiell gefährdete Unternehmen zu schützen,
- Angriffsmethoden zu erkennen,
- Angriffsziele zu ermitteln und
- Schutzmaßnahmen zu entwickeln.

innerJoin(
access

Technische Angriffspunkte

Eine zunehmend stärkere Nutzung des Internets in betrieblichen Abläufen eröffnet neben vielen Vorteilen auch neue Angriffspunkte für Wirtschaftsspione. Um ein Unternehmen auszuspionieren, muss der Täter die Geschäftsräume oder die Fabrik nicht mehr betreten. Er kann ohne großes Entdeckungsrisiko von seinem Heimatland aus versuchen, an die Unternehmensdaten zu gelangen. Aber auch für Spionage vor Ort bieten sich neue technische Möglichkeiten, um an sensible Unternehmensdaten zu gelangen.

Industrie 4.0

Gefahren

In der Industrie 4.0 verzahnt sich die Produktion auf intelligente Weise mit modernster Informations- und Kommunikationstechnik. Das bietet immense Vorteile und ermöglicht es maßgeschneiderte und kostengünstige Produkte in hoher Qualität und nach individuellen Kundenwünschen herzustellen. Nahezu alle Prozesse werden digitalisiert und miteinander vernetzt.

Mit steigendem Vernetzungsgrad wird eine Unternehmens-IT jedoch auch angreifbarer. Dringt der Täter erfolgreich an einer Stelle im System ein, erhält er möglicherweise Zugang zu anderen Bereichen, in denen sensible Unternehmensdaten gespeichert werden oder Steuerungsprozesse der Produktion zugänglich sind. Daten könnten gestohlen oder Produktionsprozesse sabotiert werden.

Das können Sie tun

Besonders gefährdet sind Schnittstellen zum Internet. Sie sollten zur Sicherheit der Unternehmensdaten im notwendigen Maße begrenzt und gesondert gesichert werden.

Zugleich müssen organisatorische Maßnahmen ergriffen werden. Netze mit unterschiedlichen Funktionen sollten beispielsweise voneinander getrennt werden. Sichern Sie Fernwartungszugänge gesondert ab und erlauben Sie externe Zugriffe nur in speziell dafür vorgesehenen Zeitfenstern.

Setzen Sie Werkzeuge ein, die den Datenverkehr überwachen. So lassen sich Angriffe oder ein Missbrauch zeitnah erkennen.

Cloud Computing

Gefahren

Cloud Computing ist sehr praktisch, aber auch sehr risikoreich. Mit Cloud-Technologie lassen sich Kosten für Speicher- und Rechenkapazitäten einsparen und Daten weltweit abrufen. Die Daten werden dazu jedoch aus dem Unternehmen ausgelagert. Sie befinden sich physikalisch nicht mehr in Ihrem Unternehmen und damit nicht mehr unter Ihrer alleinigen Kontrolle. Sie haben zwar das Wort des Betreibers der Cloud-Plattform, dass niemand Ihre Daten einsehen darf und kann. Dies können Sie jedoch nicht kontrollieren.

Das können Sie tun

Es spricht grundsätzlich nichts dagegen, Daten in einer Cloud zu hinterlegen, die nicht vertraulich sind und ohnehin in die Öffentlichkeit gelangen (beispielsweise speicherintensive Präsentationen des Vertriebs). Mitarbeiterinnen und Mitarbeiter können so von jedem Ort aus darauf zugreifen.

Sensible Unternehmensdaten gehören jedoch nicht in eine Cloud. Sie müssen unter besonderen Schutzvorkehrungen im Unternehmen verbleiben.

Mobile Geräte

Gefahren

Ziel von Angriffen ist heute nicht mehr nur die IT-Infrastruktur auf dem Gelände und in den Gebäuden eines Unternehmens. Betroffen ist vielmehr die gesamte Kommunikationsinfrastruktur.

Smartphones spielen dabei eine sehr wichtige Rolle. Jedes moderne Mobiltelefon funktioniert wie ein Computer und ist ebenso leicht angreifbar. Es ist in den meisten Fällen jedoch überhaupt nicht oder nur unzureichend geschützt.

Mit entsprechender Schadsoftware lassen sich diese Geräte so infizieren, dass sie beispielsweise wie „Wanzen“ funktionieren. Werden Sie mit in eine vertrauliche Besprechung genommen, lassen sich die Gesprächsinhalte sehr einfach an einen möglichen Angreifer übertragen. Telefonate können mitgehört und die auf dem Gerät gespeicherten Daten ausgelesen werden.

Das können Sie tun

Private Smartphones sollten nicht geschäftlich genutzt werden und keinen Zugriff auf das jeweilige Unternehmensnetzwerk erhalten. Sollte dies in Ausnahmefällen dennoch erforderlich sein, muss ein technisches Sicherheitskonzept die Rahmenbedingungen für einen solchen Zugriff definieren. Fragen des Datenschutzes sind zu beachten.

Mobile Geräte sollten niemals in vertrauliche Besprechungen mitgenommen werden.

Geben Sie Ihre Mobilfunknummer insbesondere im Ausland nur zurückhaltend weiter.

Lassen Sie mobile Geräte niemals unbeaufsichtigt liegen und schalten Sie die WLAN- und Bluetooth-Schnittstellen ab, wenn Sie sie nicht benötigen.

Übermitteln Sie beispielsweise nach einem wichtigen Meeting nicht sämtliche Inhalte der Gespräche über ein Telefon. Nutzen Sie besser mehrere Kommunikationswege.

Müssen sensible Unternehmensdaten ausnahmsweise telefonisch übermittelt werden, dann setzen Sie geeignete Verschlüsselungstechnik ein.

E-Mail Kommunikation

Gefahren

Eine bevorzugte Angriffsvariante von Wirtschaftsspionen sind E-Mails mit angehängter Schadsoftware. Es handelt sich bei dieser so genannten Malware in der Regel um sogenannte Trojaner. Sie setzen sich im Unternehmensnetzwerk fest und übertragen Unternehmensdaten an den Angreifer.

Einige Trojaner können weitere Schadsoftware nachladen. Durch die Möglichkeit zur Sabotage sind sie insbesondere für IT-gestützte Produktionsprozesse sehr gefährlich. Ein intelligent arbeitender Trojaner mit dem Namen Stuxnet hat beispielsweise über ein Jahr das iranische Atomprogramm erfolgreich sabotiert.

Für einen Angriff präparierte E-Mails sind häufig gezielt auf die jeweiligen Adressaten zugeschnitten und dadurch getarnt, dass sie sich auf die jeweiligen Tätigkeitsbereiche beziehen. Sie sind deshalb in Form und Inhalt häufig nicht oder nur äußest schwer als Fälschung zu erkennen.

Das können Sie tun

Misstrauen Sie allen E-Mails, die irgendwelche Auffälligkeiten enthalten. Hinterfragen Sie kritisch den Inhalt, den Gesamtkontext und den Zeitpunkt, zu dem Sie eine E-Mail erhalten.

Angreifern gelingt es nicht immer, die Identität eines vermeintlichen Absenders hundertprozentig zu imitieren. Haben Sie beispielsweise mit einem Kollegen ein für Ihre Arbeit relevantes Problem im Detail erörtert, ist es unwahrscheinlich, dass dieser Ihnen einen Tag später eine E-Mail dazu ins Büro schickt.

Ein Unternehmensnetzwerk sollte organisatorisch aber auch so eingerichtet und gesichert sein, dass im Fall des Eindringens von Schadsoftware diese dort keinen erheblichen Schaden anrichten kann. Teilen Sie das Netzwerk daher beispielsweise in voneinander unabhängige Teilbereiche auf und erstellen Sie in kurzen Intervallen Sicherungskopien aller relevanten Daten. Vertrauen Sie nicht blindlings auf den Backup-Prozess, sondern üben Sie regelmäßig auch das Wiederherstellen gesicherter Daten. Es wäre dramatisch, wenn Sie im Ernstfall statt der Sicherung nur einen leeren oder fehlerhaften Speicherbereich vorfänden.

USB-Speicher

Gefahren

USB-Sticks enthalten nicht immer nur Daten. Es können auch schädliche Programme auf diesen Datenträgern gespeichert sein. Wird ein mit einem Schadprogramm infizierter USB-Stick an einen Computer angeschlossen, kann die Schadsoftware unbemerkt auf den Rechner und von dort in das gesamte Unternehmensnetzwerk gelangen. Eine solche Übertragung von Malware ist in wenigen Sekunden möglich. USB-Sticks werden häufig gezielt für Angriffe auf Unternehmensnetzwerke eingesetzt.

Das können Sie tun

Prüfen Sie genau, ob das Anschließen von USB-Speichermedien an Rechner im Unternehmensnetzwerk erlaubt sein soll. Geeignete organisatorische Maßnahmen, wie der Einsatz von dezentralen und besonders gesicherten Schleusenrechnern, können die Gefahren auf ein Mindestmaß reduzieren. Dort lassen sich auch andere Datenträger wie beispielsweise CD-ROMs einlesen.

Sperren Sie bei allen übrigen Rechnern die USB-Anschlüsse so, dass eine Infizierung mit Schadsoftware auf diesem Weg ausgeschlossen ist. Es empfiehlt sich eine vollständige Sperrung der Ports, da es USB-Sticks auf dem Markt gibt, die vortäuschen, es würde eine Tastatur angeschlossen.

Müssen im Unternehmen Daten von USB-Sticks ausgelesen werden, sollte dies entweder an Rechnern erfolgen, die nicht mit dem Netzwerk verbunden sind, oder nach eingehender Überprüfung des Mediums durch die IT-Abteilung.

Keylogger

Gefahren

Keylogger zeichnen sämtliche Tastatureingaben auf, also auch die Eingabe von Benutzernamen und Passwörtern.

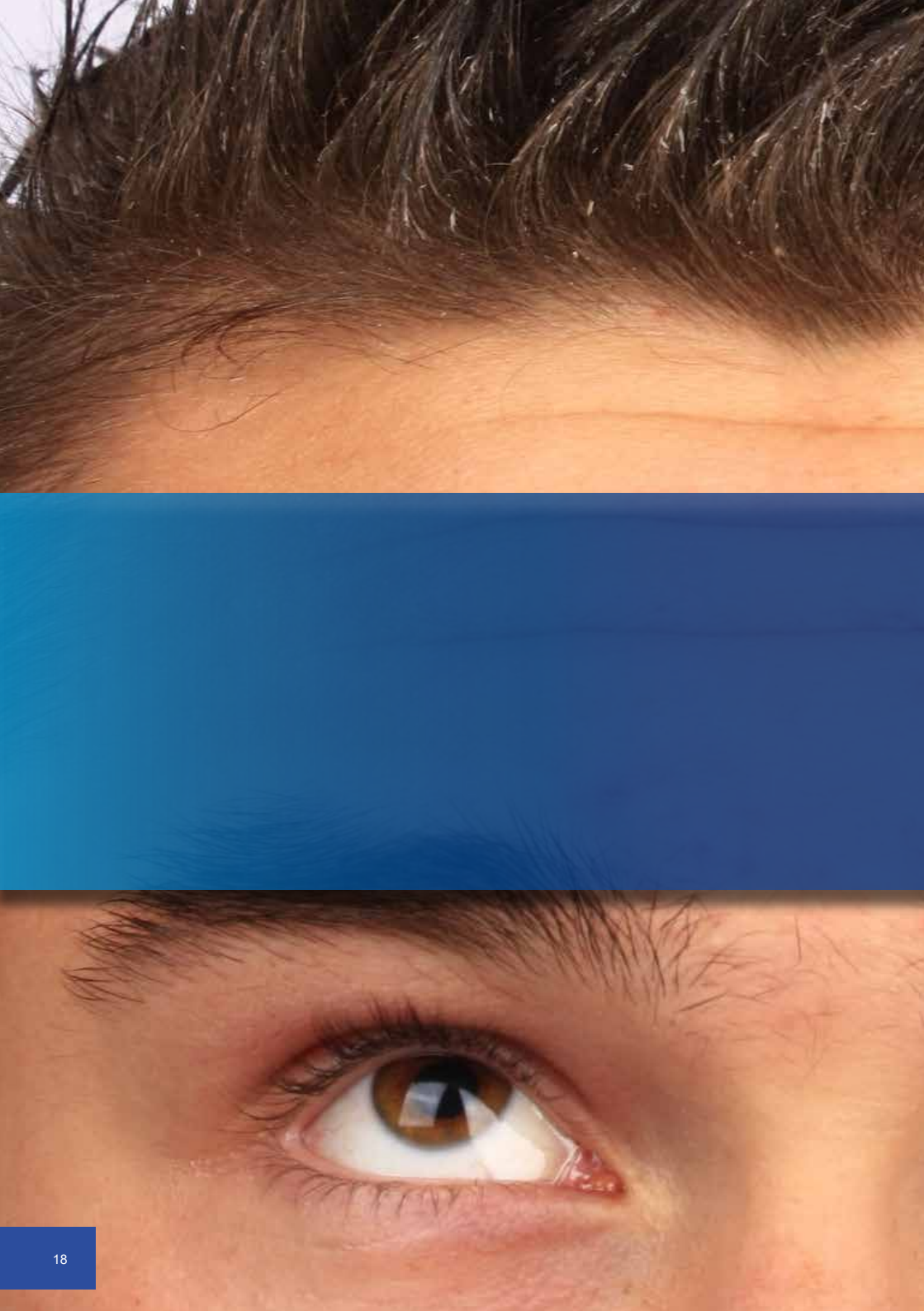
Es gibt grundsätzlich zwei Varianten: Keylogger-Software kann über infizierte E-Mail-Anhänge oder auch über USB-Sticks in ein IT-Netzwerk eingeschleust werden. Hardware-Keylogger sehen aus wie kleine Stecker und werden zwischen Tastatur und den Arbeitsplatzrechner geklemmt. Dazu muss der Angreifer zumindest kurzfristig Zugriff auf den betreffenden Computer im Unternehmen haben. Selbst technisch unerfahrene Menschen können Keylogger in Sekundenschnelle anschließen.

Es gibt Fälle, in denen sich Angreifer als Techniker, Reinigungspersonal oder Handwerker ausgeben, um Keylogger unverdächtig in Büros anzubringen.

Das können Sie tun

Häufig werden Keylogger über den Anhang von E-Mails in ein Unternehmensnetzwerk eingeschleust. Legen Sie daher Regeln für den sicheren Umgang mit elektronischen Nachrichten fest und sensibilisieren Sie alle Beschäftigten zu diesem Thema.

Vor Hardware-Keyloggern können Sie sich wirksam schützen, indem Sie Unbefugten keinen Zugang zu entsprechenden Rechnern ermöglichen. Stellen Sie sicher, dass Büros verschlossen sind, wenn sich dort niemand aufhält. Lassen Sie Besucher oder Fremdpersonal niemals unbeaufsichtigt in der Nähe von Computern arbeiten.



Sicherheitsrisiko Mensch

Sehr viele Lücken in der Sicherheitsarchitektur werden durch das Verhalten von Menschen geschaffen. Beispielsweise werden ungewöhnliche E-Mails sorglos geöffnet oder gefundene USB-Sticks bedenkenlos an den Firmenrechner angeschlossen. Dabei muss keine böse Absicht im Spiel sein. Meist wird leichtsinnig gehandelt und Sorgfaltspflichten werden außer Acht gelassen. Angreifer wissen um die „Schwachstelle Mensch“, die sie immer wieder gezielt für das Ausspionieren von Unternehmen nutzen.

Social Engineering

Gefahren

Beim Social Engineering nutzen Angreifer gezielt menschliche Schwächen sowie die Arglosigkeit von Personen aus, um insbesondere Zugriff auf die IT-Systeme von Unternehmen zu erhalten.

Weil der technische Schutz von Systemen verbessert und Angriffe auf IT-Infrastrukturen dadurch erschwert werden, nutzen Angreifer nicht mehr ausschließlich ihre technischen Möglichkeiten. Die Zahl der Angriffe auf sensible Daten oder das Know-how von Unternehmen mit Hilfe von Social Engineering steigt stark an.

Unternehmensbeschäftigte werden beispielsweise auf Messen oder Veranstaltungen gezielt angesprochen. Im Vorfeld werden in sozialen Netzwerken persönliche Informationen zum ausgewählten Gesprächspartner recherchiert. Mit diesem Wissen im Hintergrund wird die Unterhaltung beispielsweise auf einen angeblichen Forschungsauftrag oder auf vermeintlich interessante und lukrative Berufsperspektiven gelenkt.

Wussten Sie, dass ...

der Verfassungsschutz NRW kostenlose Awareness-Vorträge in Ihrem Unternehmen hält? Sprechen Sie uns gerne an!

Das können Sie tun

Halten Sie sich mit Auskünften zurück

Social Engineering verfolgt das Ziel, widerrechtlich an Informationen zu gelangen. Dabei wird häufig eine falsche Identität vorgetäuscht. Durch eine ausgefeilte Gesprächsführung und ein entsprechendes Auftreten soll man dazu verleitet werden, etwa in einer angenehmen und kollegialen Plauderei Interna des Unternehmens preiszugeben.

Geben Sie immer nur Auskünfte, zu denen sie ausdrücklich befugt sind und die im Kontext der Frage notwendig sind. Das gilt auch für auf den ersten Blick vermeintlich unwichtige Informationen über Zuständigkeiten oder persönliche Informationen über Kolleginnen und Kollegen. Dies sind häufig nützliche Puzzlestücke für eine nächste Stufe des Angriffes.

Lassen Sie Sicherheit vor Höflichkeit walten

Angreifer versuchen bewusst, Situationen zu schaffen, in denen Sie kurzfristig entscheiden müssen, ob und welche Informationen Sie preisgeben. Dann gilt es, einen kühlen Kopf zu bewahren. Nehmen Sie sich Zeit, eine Situation nüchtern zu analysieren. Sagen Sie beispielsweise einen Rückruf zu und halten Sie Rücksprache in Ihrem Unternehmen. Hier geht Sicherheit vor Höflichkeit.

Sorgen Sie für Awareness im Unternehmen

Sicherheit ist ein von der Unternehmensspitze ausgehender, übergreifender Prozess. Es ist wichtig, dass Mitarbeiterinnen und Mitarbeiter das Thema Wirtschaftspionage und aktuelle Angriffsvarianten kennen. Führen Sie regelmäßige und umfassende Sensibilisierungsmaßnahmen im Unternehmen durch.

Auslandsreisen

Gefahren

Bei Reisen ins Ausland haben die dortigen Nachrichtendienste „Heimvorteil“. Sie kommen leichter an mitgeführte Unternehmensdaten. Gesetze des jeweiligen Staates können Nachrichtendienste dazu ermächtigen, die von Ihnen mitgeführten Unternehmensdaten zu entwenden.

Bereits einfache Verstöße gegen Regelungen im Reiseland können von den dortigen Behörden als Druckmittel genutzt werden. Was in Deutschland ein Bagatelldelikt ist, kann in einem anderen Staat Geschäftsreisende vor die Wahl stellen, mit einem fremden Nachrichtendienst zu kooperieren oder aber inhaftiert zu werden.

Das können Sie tun

Machen Sie sich mit den Bestimmungen des jeweiligen Landes genau vertraut und beachten Sie diese, selbst wenn sie Ihnen absurd erscheinen.

Vermeiden Sie alle Situationen, die zu Erpressungsversuchen führen könnten. Bleiben Sie nach Möglichkeit in Ihrer Freizeit im Hotel oder besuchen Sie ausschließlich touristische Ziele.

Führen Sie wichtige Dokumente und mobile Geräte wie Smartphone, Laptop oder Tablet stets bei sich. In Hotelsafes sind Ihre Daten nicht sicher. Hotels kooperieren in vielen Ländern mit Nachrichtendiensten.

Nutzen Sie alle zur Verfügung stehenden technischen Sicherheitsmaßnahmen für Ihre Daten. Klären Sie aber vor der Geschäftsreise unbedingt, ob Verschlüsselung und Passwortschutz im Zielland erlaubt sind.

Beschränken Sie Ihre vertrauliche Kommunikation auf ein absolut notwendiges Maß.

Nutzen Sie nach Möglichkeit für Dienstreisen ins Ausland sogenannte „nackte“ Laptops oder Smartphones, auf denen Sie nur die für diese Reise unbedingt notwendigen Daten mitführen. Kontrollieren Sie die Geräte nach Rückkehr auf Schadsoftware. Der sicherste Weg: Schließen Sie im Ausland mitgeführte Informations- und Kommunikationstechnik nicht mehr an das Unternehmensnetzwerk an und nutzen Sie sie nicht mehr für Unternehmenszwecke.

Fahrlässiger Umgang mit Daten

Gefahren

Ein fahrlässiger Umgang mit sensiblen Unternehmensdaten kann ernsthafte wirtschaftliche Folgen haben. Die folgenden Situationen sind beispielweise häufig anzutreffen:

- Mobilgeräte werden in Taxis, an Flughäfen oder Bahnhöfen liegen gelassen.
- In öffentlichen Verkehrsmitteln werden sensible Unternehmensinterna laut am Telefon besprochen.
- Vertrauliche Schriftstücke werden in der Öffentlichkeit auf dem Notebook angeschaut und können über die Schulter oder von der Seite mitgelesen werden.
- In der Lounge eines Bahnhofs oder Flughafens wird das eigene Laptop unbeaufsichtigt stehen gelassen, während man sich nur kurz einen Kaffee holt.
- Zwischen Home-Office und Unternehmen werden Daten ungeschützt übermittelt.

Obwohl die meisten Menschen wissen, dass ein solches Verhalten zu einem Abfluss von Unternehmensdaten führen kann, wird nicht immer die notwendige Sorgfalt an den Tag gelegt.

Das können Sie tun

Handeln Sie bewusst. Machen Sie sich klar, welche Folgen fahrlässiges Handeln für Ihr Unternehmen haben kann. Der unsichere Weg scheint manchmal der einfachere zu sein. Die Erfahrung zeigt jedoch, dass dadurch das Risiko deutlich steigt.

Entwickeln Sie Sicherheitsrichtlinien für Ihr Unternehmen. Machen Sie deren Umsetzung zur Chefsache. Vermitteln Sie dabei, dass es keine Vorschriften sind, die das Ziel haben, Beschäftigte in ihrem Handeln einzuschränken. Sie beruhen vielmehr auf Erfahrungen aus realen Angriffen und dienen dem Schutz Ihres Unternehmens.

Ganzheitliches Sicherheitskonzept

Sicherheit im Unternehmen ist immer ganzheitlich zu betrachten. Es geht um mehr als reine IT-Sicherheit. Unternehmenssicherheit gehört in professionelle Hände und sollte von einer eigenen Organisationseinheit (Corporate Security) bearbeitet werden. In dieser Organisationseinheit sollten alle Sicherheitsprozesse des Unternehmens verantwortet und verzahnt werden. Sicherheit selbst ist für sich gesehen kein wertschöpfender Vorgang, jedoch schützt sie die Unternehmenswerte und flankiert die Gewinnerzielung. Sie ist somit ein wichtiger Wettbewerbsvorteil.

In vier Schritten zum ganzheitlichen Sicherheitskonzept

Mit den folgenden vier Schritten begeben Sie sich auf den Weg zu einem erfolgreichen ganzheitlichen Sicherheitskonzept:

1. Schutzbedarf festlegen
Identifizieren Sie das absolut schützenswerte Know-how und die sensiblen Daten Ihres Unternehmens. Was darf auf keinen Fall in die Hände der Konkurrenz geraten, weil der Verlust gegebenenfalls sogar existenzbedrohend sein könnte? In der Regel sind dies nicht mehr als fünf Prozent aller Unternehmensdaten. Die übrigen Daten sind ohnhin zu großen Teilen auf Grund rechtlicher oder vertraglicher Verpflichtungen offenzulegen.

2. Standorte/Aufbewahrungsorte erfassen
Prüfen Sie, auf welchen Servern, in welchen Panzerschränken oder Produktionshallen das absolut schützenswerte Know-how im Unternehmen zu finden ist. Sämtliche Aufbewahrungsorte müssen bestmöglich vor möglichen Angreifern gesichert werden.

3. Betroffene Arbeitsplätze identifizieren
Tragen Sie zusammen, welche Mitarbeiterinnen und Mitarbeiter mit dem absolut schützenswerten Know-how im Unternehmen arbeiten.

4. Schutzring ziehen
Ziehen Sie einen Schutzring aus den drei folgenden Komponenten um die betroffenen Arbeitsplätze:

Organisation - Informieren Sie die Mitarbeiterinnen und Mitarbeiter darüber, dass sie täglich mit dem absolut schützenswerten Know-how des Unternehmens arbeiten. Geben Sie ihnen verbindliche Regelungen an die Hand, wie sie das Kern-Know-how zu schützen haben.

Technik - Halten Sie Ihr Unternehmen insbesondere im Bereich der IT-Sicherheit stets auf dem neuesten Stand. Verschlüsselung von Daten, ein funktionierendes Patchmanagement, Monitoring des IT-Netzwerkes und aktuellste Sicherheitssoftware sollten als Bestandteile des IT-Sicherheitsmanagements selbstverständlich sein. Sichern Sie die Bereiche, in denen die „Kronjuwelen“ des Unternehmens aufbewahrt werden, durch besondere technische Vorkehrungen.

Awareness - Sensibilsieren Sie Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig für die Gefahren, die Angreifer und ihre Methoden.

Verfassungsschutz als Ansprechpartner

Benötigen Sie eine präventive Beratung oder Unterstützung für den Fall, dass Ihr Unternehmen Opfer eines Angriffs geworden ist? Dann wenden Sie sich vertrauensvoll an den nordrhein-westfälischen Verfassungsschutz.

Der Verfassungsschutz ist ein kompetenter Partner für Wirtschaftsschutz und die Abwehr von Wirtschaftsspionage. Wir bieten Ihnen eine vertrauliche Zusammenarbeit an und nehmen beispielsweise Rücksicht auf das Interesse eines Unternehmens, einen Imageschaden zu vermeiden.

Sie erreichen uns
per E-Mail unter **wirtschaftsschutz@im1.nrw.de**
und telefonisch unter **0211 871 2821**.

Wussten Sie, dass ...

der Wirtschaftsschutz im nordrhein-westfälischen Verfassungsschutz kostenlose Initialberatungen anbietet? Damit hilft er Unternehmen, Handlungsfelder zu identifizieren und zu priorisieren.

Unternehmen in NRW können sich gerne mit ihren Fragen zu Sicherheitskonzepten und Unternehmenssicherheit ans uns wenden. Der gemeinsame Austausch ist wichtig, um für mehr Sicherheit zu sorgen.

Auf Wunsch berät Sie der Verfassungsschutz vor Ort in Ihrem Unternehmen. Zusätzlich bieten wir Vorträge an, die zu Angreifern und deren Strategien sensibilisieren und über Grundsätze zum Schutz der Wirtschaft vor Spionage, Sabotage oder Datendiebstahl informieren.

Hinweis

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit des Ministeriums des Innern des Landes Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlbewerberinnen und Wahlbewerbern oder Wahlhelferinnen und Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für die Landtags-, Bundestags- und Kommunalwahlen sowie für die Wahl der Mitglieder des Europäischen Parlaments. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt.

Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme des Ministeriums des Innern Nordrhein-Westfalen zugunsten einzelner politischer Gruppen verstanden werden könnte.

Der Inhalt dieser Broschüre wurde auf chlorfrei gebleichtem Papier gedruckt.

Impressum

Herausgeber
Ministerium des Innern
des Landes Nordrhein-Westfalen
Friedrichstraße 62-80
40217 Düsseldorf

Telefon: 0211/871-01
Telefax: 0211/871-3355
poststelle@im.nrw.de
www.im.nrw

Redaktion
Verfassungsschutz Nordrhein-Westfalen
Telefon: 0211/871-2821
Telefax: 0211/871-2980

kontakt.verfassungsschutz@im1.nrw.de

Bestellservice
bestellung.verfassungsschutz@im1.nrw.de
www.im.nrw/broschueren-des-verfassungsschutzes
Stand: September 2022

Fotos:
fotolia.com - Denys Rudyi, Dmitry Nikolaev, industrieblick, vege, imagecore, psdesign1, BlueSkyImages, vivjanna13, Rawpixel.com, Robert Kneschke
Shutterstock.com - Shaynepplstockphoto, Leonardo da
Verfassungsschutz Nordrhein-Westfalen

Ministerium des Innern
des Landes Nordrhein-Westfalen
Friedrichstraße 62 - 80
40217 Düsseldorf

Telefon: 0211/871 - 01
Telefax: 0211/871 - 3355
kontakt.verfassungsschutz@im1.nrw.de
www.im.nrw