sosafe

Die IT-Bedrohungslage im öffentlichen Sektor

Aktuelle Gefahren für deutsche Organisationen und wie Sie sich schützen können

Die Zahl der Cybervorfälle ist in den letzten Jahren stark gestiegen, auch im öffentlichen Sektor. Kritische Infrastrukturen werden gezielt angegriffen – mit weitreichenden Konsequenzen. Krankenhäuser, Regierungsbehörden, die öffentliche Verwaltung, Versorgungsunternehmen und Militäreinrichtungen müssen sich jetzt mit effektiven Maßnahmen wappnen und für die Zukunft sicher aufstellen.

Die aktuelle Lage

98%

der Unternehmen des öffentlichen Sektors waren im vergangenen Jahr **von KI-gestützten Cyberangriffen betroffen.**

Quelle: SoSafe 2024

96%

der Sicherheitsexperten im öffentlichen Sektor glauben, dass die **Lücke in der Cybersicherheit immer größer** wird.

Quelle: SoSafe 2024

68%

der Sicherheitsverstöße sind auf den **Faktor Mensch** zurückzuführen.

Quelle: Verizon, 2024

Die Frage lautet nicht, ob eine Organisation angegriffen wird, sondern wann – das gilt nicht nur für Privatunternehmen, sondern auch im öffentlichen Sektor.

Kritische Infrastrukturen im Visier

Die Beweggründe für Angriffe auf den öffentlichen Sektor sind vielfältig: Erbeutung oder Zerstörung von Daten, Betriebsunterbrechungen, öffentliche Sichtbarkeit, finanzieller Gewinn oder Spionage. Wir beobachten zunehmende Angriffe insbesondere auf die kritischen Infrastrukturen:

- **Krankenhäuser**
- **Regierungsbehörden**
- **Kommunalverwaltungen**
- **Versorgungsunternehmen**
- **Militäreinrichtungen**
- **Bildungseinrichtungen**
- **Justizbehlrden**

Angriffe auf die Systeme solcher Organisationen haben weitreichende Konsequenzen, die weit über die Unterbrechung von Diensten hinausgehen. Werden kritische Infrastrukturen kompromittiert, kann es zu politischem Aufruhr und sogar zur Gefährdung von Menschenleben kommen. Hinzu kommen kostspielige und zeitintensive Wiederherstellungsprozesse, die öffentliche Budgets belasten und das Vertrauen der Öffentlichkeit schwächen.

Die größten Gefahren

Ransomware-Angriffe durch Hackergruppen sind nach wie vor die größte Gefahr. Die Schadsoftware verschlüsselt alle Daten und häufig auch Backups. Das kann grundlegende Dienste des öffentlichen Sektors zum Stillstand bringen.

Behörden, Versorgungsunternehmen und Gesundheitseinrichtungen sind beliebte Opfer staatlich finanzierter Cyberangriffe. Werden deren Systeme unterbrochen, kann das die nationale und öffentliche Sicherheit direkt bedrohen.

Hacktivisten greifen Regierungsorganisationen an, um aus sozialem und politischem Aktivismus Gesetzgebungsprozesse zu stören.

Der erste Angriffspunkt sind oft Phishing-E-Mails: Mitarbeitende werden mit ausgefeilten Methoden dazu gebracht, auf gefährliche Links zu klicken, Anhänge zu öffnen oder sensible Informationen zu verraten.

Sicherheitslücken, die die Angreifer ausnutzen, sind in den teils veralteten Systemen des öffentlichen Sektors oft zahlreich vorhanden und können von unterbesetzten IT-Teams mit unzureichenden Budgets nicht schnell genug geschlossen werden.

KI macht zielgerichtete Angriffe auf Menschen immer leichter: Auf Knopfdruck werden überzeugende betrügerische E-Mails massenhaft erstellt, Ton- und sogar Videoaufnahmen echter Personen lassen sich täuschend echt fälschen.

> Die Zusammenarbeit zwischen privatem und öffentlichem Sektor ist unerlässlich. Nicht umsonst heißt es "Es braucht ein internationales Netzwerk, um ein internationales Netzwerk zu besiegen."
>
> **Philipp Amann**
> Group CISO, Österreichische Post AG

Finanzielle Verluste in Millionenhöhe

2,5 Millionen Euro

Entstanden durch den Ransomware Angriff auf den Landkreis Anhalt-Bitterfeld.

Quelle: DSGVO

Ein Cyberangriff verursacht hohe Kosten, die sich schnell bis in den siebenstelligen Bereich summieren. Eine Beispielrechnung für eine Klinik:

200.000 €	für die Systemwiederherstellung durch IT-Dienstleister
350.000 €	entgangene Einnahmen durch verschobene Behandlungenschon bei 2 Tagen Betriebsunterbrechung
100.000 €	Lösegeldzahlung
250.000 €	Haftungskosten und Bußgelder wegen Datenschutzverletzungen
300.000 €	Kosten durch verlorenes Vertrauen und Umsatzverlust

= 1,2 Millionen €

Es kann jeden treffen

Cyberkriminelle nehmen keine Rücksicht darauf, welche Folgen ihre Handlungen für die Gesellschaft haben. Behörden und Versorgungsunternehmen werden genauso angegriffen wie Kliniken und sogar NGOs.

2020:
Ausgehend von Phishing-E-Mails wird das Universitätsklinikum Düsseldorf Opfer von Ransomware. Die IT-Systeme des Krankenhauses sind mehrere Wochen lahmgelegt, die finanziellen Verluste erheblich. Vor allem aber wird die Patientenversorgung beeinträchtigt – eine Patientin verstirbt, da sie aufgrund des Angriffs nicht rechtzeitig behandelt werden kann.

2021:
Der Landkreis Anhalt-Bitterfeld wird mit Ransomware angegriffen, die über einen Trojaner in die IT-Systeme der Verwaltung gelangt. 20 Ämter sind nicht mehr arbeitsfähig. Die digitale Korrespondenz kommt zum Erliegen, Bafög und Wohngeld können nicht mehr ausgezahlt werden. Der Katastrophenfall wird ausgerufen und dauert mehr als ein halbes Jahr an. Insgesamt kostet der Vorfall 2,5 Millionen Euro.

2023:
Ein kommunaler IT-Dienstleister wird Opfer eines Ransomware-Angriffs und muss daraufhin die Verbindung zu allen Kommunen kappen, die er mit IT-Infrastruktur bedient. 22.000 Arbeitsplätze sind weitestgehend offline und insgesamt 1,6 Millionen Bürger:innen von den Folgen des Angriffs betroffen. Der Krisenmodus des Dienstleisters dauert 11 Monate an. In dieser Zeit wendet die Belegschaft allein für die Bewältigung der Krise rund 43.000 Arbeitsstunden auf.

Von diesen Beispielen gibt es unzählige weitere.
Auf der Website kommunaler-notbetrieb.de wird das ganz Ausmaß deutlich.

IT-Sicherheitsvorfälle in Kommunalverwaltungen seit 2010

NIS2 kommt

Organisation jetzt gegen Cyberangriffe wappnen. Damit erfüllen Sie gleichzeitig diverse Regularien, die den öffentlichen Sektor zur Verbesserung seiner Resilienz verpflichten –aktuell insbesondere die NIS2.

Die **NIS2-Richtlinie der EU** soll angesichts wachsender Cybergefahren die Sicherheit und den Schutz kritischer Infrastrukturen in den Mitgliedsländern stärken. Dafür legt sie für kritische Sektoren strengere Cybersicherheitsstandards fest. Typische Bereiche umfassen unter anderem die öffentliche Sicherheit, den Energiesektor und das Gesundheitswesen.

Sobald das deutsche NIS2-Umsetzungsgesetz in Kraft tritt, bleibt nicht mehr viel Zeit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät Organisationen, sich bereits jetzt auf die NIS2-Regulierung vorzubereiten, indem sie ihre Informationssicherheit verbessern und konkrete technisch-organisatorische Maßnahmen umsetzen. Dazu gehört ganz zentral auch ein effektives Risikomanagement. In den Artikeln 7, 9, 20 und 21 wird die Wichtigkeit von Schulungen sowohl für Leitungsorgane als auch für die Mitarbeitenden betont.

Der Mensch ist der entscheidende Faktor

Der überwiegende Teil der Sicherheitsvorfälle beginnt mit dem Menschen als Einfallstor – häufig ein schädlicher Link oder Anhang in einer E-Mail. Deshalb liegt das größte Potenzial für mehr Sicherheit und Resilienz bei den Menschen in Ihrer Organisation.

Wie Hacker angreifen

Angreifer machen sich gezielt die **menschliche Psyche** zunutze und werden dabei immer ausgeklügelter.

Sie setzen beispielweise auf Neugier, indem sie brisante Informationen versprechen. Sie machen Druck, oder nutzen Hilfsbereitschaft aus. Sie arbeitet mit Autorität, wenn sie sich als Vorgesetzte ausgeben, manipulieren über Schmeichelei und stellen durch vermeintliche Gemeinsamkeiten Vertrauen her.

Das sind die häufigsten Methoden:

Phishing (von engl. fishing, „angeln"):
Über präparierte E-Mails, Nachrichten oder Anrufe werden Mitarbeitende dazu verleitet, vertrauliche Informationen preiszugeben, die für Angriffe nützlich sind. So werden beispielsweise Zugangsdaten, PIN-Codes und Geschäftsgeheimnisse „abgefischt".

Social Engineering (in etwa „soziale Manipulation"):
Mit Beeinflussungstechniken werden Menschen zu einem bestimmten Verhalten bewegt. Ein Angreifer könnte sich beispielsweise als Geschäftsführer ausgeben und mit einer plausibel klingenden Geschichte eine Mitarbeiterin veranlassen, Geld vom Firmenkonto auf sein eigenes zu überweisen.

Wie Sie sich schützen können

1. Wissen vermitteln:

Das BSI empfiehlt praxisnahe Schulungen. Mit personalisierten, realitätsnahen Awareness-Trainings schaffen Sie das notwendige Bewusstsein, um Ihre Organisation zu schützen. **Ihre Mitarbeitenden lernen, potenzielle Bedrohungen zu erkennen und sich sicher im digitalen Raum zu bewegen.**

Wichtig ist dabei nicht nur der fachlich korrekte, gut verständliche Inhalt. Die Schulungen müssen auch mit **wenig Aufwand** in den Arbeitsalltag integrierbar sein – und vor allem **Spaß mache**n. Spielerische Inhalte fördern nachhaltige Verhaltensänderungen und schließen gezielt Wissenslücken.

Zur Unterstützung **des langfristigen Lernerfolgs** können Sie selbst **einiges tun**, um Ihre Mitarbeitenden zum Lernen zu motivieren:

- Individuelle Lernpfade nutzen, die auf die Prioritäten Ihrer Organisation ausgerichtet ist, und Pflichtmodule festlegen. Das gibt Orientierung, und Ihre Mitarbeitenden verstehen, was die Inhalte mit ihrer eigenen Arbeit zu tun haben.

- Regelmäßig erinnern. Das geht am zeitsparendsten mit automatisierten E-Mails. Auch eine individuelle Überwachung des Lernfortschritts ist möglich, sodass Sie einzelne Mitarbeitende gezielt ermuntern können.

- IT-Sicherheit zur Chefsache machen. Verdeutlichen Sie, dass das Thema alle etwas angeht und auch die Geschäftsführung mit vollem Einsatz dabei ist.

2. Wissen anwenden und üben:

Neues Wissen festigt sich erst dann, wenn es regelmäßig angewendet wird. Das BSI empfiehlt dafür **Phishing-Simulationen**. Sie stellen Cyberangriffe realitätsnah nach, um Mitarbeitende für die Gefahren solcher Attacken zu sensibilisieren und ihnen **sicheres Verhalten anzutrainieren**.

Um häufige Fallstricke zu vermeiden, können Sie sich an **folgende Tipps und Best Practices** halten. Sie sorgen für effektive Simulationen, die das sichere Verhalten Ihrer Mitarbeitenden fördern und eine schützende Sicherheitskultur in Ihrer Organisation etablieren:

- IT-Systeme auf die Phishing-Simulation vorbereiten, damit die simulierten E-Mails nicht im Spam-Ordner landen, und mit Testversänden bereits im Vorfeld prüfen, ob alles wie vorgesehen funktioniert.

- Maßnahme ankündigen, um den Zweck zu erklären, Verunsicherung bei den Empfängerinnen und Empfängern zu vermeiden und ihre Lernmotivation zu steigern.

- Simulationen anonym durchführen, um Angst vor Schuldzuweisung zu verhindern und die Lernbereitschaft der Mitarbeitenden zu fördern.

- Schwierigkeitsgrad variieren: leicht erkennbare Mails, die Erfolgserlebnisse verschaffen, mit schwierigeren mischen, die die ausgeklügelten Taktiken echter Angriffe widerspiegeln – immer angepasst an die Kenntnisse und Anforderungen der Nutzenden.

- Simulationen mit passenden Lerninhalten begleiten, die direkt beim Klick auf eine Mail angezeigt werden, zum Beispiel in Form von Kurzvideos oder Erklärungen.

- Meldekette etablieren, damit die Empfängerinnen und Empfänger wissen, an wen sie sich im Fall der Fälle wenden sollen.

- Kontinuierlich über eine längere Zeit durchführen statt nur punktuell, um den Lernerfolg nachhaltig zu sichern.

- Unterschiedliche Phishing-Mails nach dem Zufallsprinzip versenden, damit die Ergebnisse von Anfang an aussagekräftig sind, sich der Arbeitsaufwand für den IT-Support über den gesamten Zeitraum verteilt – und anders als beim gleichzeitigen Versand identischer Mails sich die Neuigkeit nicht so schnell herumsprechen kann.

- Zwischenstände an die Nutzenden kommunizieren, damit die Mitarbeitenden ihre Leistung einschätzen können – dabei auf Verständlichkeit achten und auf positives Feedback fokussieren.

3. Erfolge messen:

Phishing-Simulationen festigen das erworbene Wissen der Mitarbeitenden und sind für Organisationen eine Möglichkeit, den Lernerfolg anhand konkreter Zahlen zu messen. Das sind die wichtigsten Kennzahlen:

- Klickrate/Interaktionsrate: Wie haben Ihre Mitarbeitenden mit den simulierten Mails interagiert, wie viele haben auf den Link geklickt?
- Melderate: Wie viele Personen haben die Phishing-Mails gemeldet, z. B. über einen Melde-Button?
- Time-to-Reporting: Wie viel Zeit verging, bis Mitarbeitende die Mails gemeldet haben?

Die Ergebnisse werden analysiert und ausgewertet, um eventuelle Wissenslücken zu erkennen. Diese können anschließend gezielt geschlossen werden, ohne das gesamte Training noch einmal wiederholen zu müssen. Ordnen Sie die Kennzahlen am besten auch nach Standort, Rolle und Funktion ein, um das Risikolevel einzelner Bereiche zu analysieren und noch individueller nachschulen zu können.

> Im Krisenfall hilft dir keine Technik, da helfen dir nur resiliente Kolleginnen und Kollegen, die eben auch in so einer Stresssituation einen kühlen Kopf bewahren, das Erlernte anwenden und ihr Bestes geben, um das Unternehmen schnell wieder auf Kurs zu bringen, SoSafe ist der Anbieter, der uns dabei hilft, schnell ans Ziel zu kommen und unsere Mitarbeitenden auf ansprechende Art und Weise einzubinden.“
>
> **Jens Feistel**
> CISO DEW21, Versorgungsunternehmen (Energie)

Wer ist sosafe ?

Aus Deutschland

Die 2018 gegründete SoSafe GmbH hat ihren Sitz in Köln. Wir sind die erste Wahl für den öffentlichen Sektor mit über 1.000 Kunden, darunter Stadtverwaltungen, Kliniken und Versorgungsunternehmen.

Psychologisch fundiert

Wir fokussieren uns darauf, Risiken ganzheitlich zu minimieren, indem wir sicheres Verhalten fördern. Deshalb basiert unsere Plattform auf den neuesten psychologischen Erkenntnissen – in unserer Produktorganisation haben über 30 % der Teammitglieder einen Hintergrund in Sozialwissenschaften oder Psychologie.

Umfassend zertifiziert

Unsere E-Learning-Plattform ist von unabhängigen Sicherheitsexperten zertifiziert. Sie erfüllt vielfältige Sicherheitsframeworks und passt sich kontinuierlich an neue Cybersicherheits-Standards an. So gewährleisten wir, dass Sie stets auf dem neuesten Stand der rechtlichen Anforderungen sind.

Die SoSafe-Plattform ist außerdem zertifiziert barrierefrei gemäß WCAG 2.1 AA & EN 301 549 und unterstützt Sie damit bei der Umsetzung des Barrierefreiheitsstärkungsgesetzes (BFSG).

Vereinbaren Sie einen Termin, um sich persönlich beraten zu lassen. Unser Expertenteam steht Ihnen gern zur Verfügung. tion ein, um das Risikolevel einzelner Bereiche zu analysieren und noch individueller nachschulen zu können.

Jetzt Termin vereinbaren

Ihr zuverlässiger Partner für die Compliance mit Sicherheitsstandards

Unsere Trainingsplattform wird zertifiziert durch unabhängige Sicherheitsexperten. Sie erfüllt vielfältige Sicherheitsframeworks und passt sich kontinuierlich an neue Cybersicherheits-Standards an. So gewährleisten wir, dass Sie stets auf dem neuesten Stand der Compliance-Anforderungen sind.

- GDPR
- NIS2
- DORA
- DIN SPEC 27076
- TISAX
- ISO 27001
- BaFin
- FCA
- PCI-DSS
- NIST
- CICIC12
- VDS 10000