Achtung: Diese Cyber-Bedrohungen lauern 2026

Cybersicherheit hat sich in den letzten Jahren so rasant entwickelt wie nie zuvor.

KI-gestützte Angriffe, immer gezielter agierende Cyberkriminelle sowie striktere Anforderungen an Datensouveränität und -hoheit verändern die Security-Landschaft grundlegend. Gegen welche Cyber-Gefahren müssen sich IT-Teams 2026 wappnen? Wie nutzen sowohl Angreifende als auch Security-Expertinnen und -Experten KI? Und was müssen Schweizer Unternehmen jetzt über Datensicherheit in der Cloud wissen?

Diesen Fragen sind wir im Gespräch mit Nadir Jabiyev, Head of IT-Security bei Xelon, nachgegangen. Nadir Jabiyev hat über 20 Jahre Erfahrung in der IT und neben Führungspositionen in IT-Sicherheit runden Stationen in System Engineering und FinTech-Compliance sein Profil ab. Im Interview ordnet er ein, was in puncto Cybersicherheit dieses Jahr auf Schweizer IT-Führungskräfte zukommt.

xelon

«Die letzten zwei Jahre haben ein Bedrohungsumfeld hervorgebracht, das schneller, präziser und strategisch schädlicher ist als je zuvor.»

— Nadir Jabiyev

Nadir, du bist seit über 20 Jahren in der IT und Head of IT-Security bei Xelon. Wie hat deine IT-Karriere begonnen und wie bist du zu Cybersicherheit gekommen?
Ich bin vor über zwanzig Jahren in die IT eingestiegen. Dies war zu einer Zeit, in der Cybersecurity noch kein klar abgegrenztes Fachgebiet war. Rollen wie Security Engineer oder Cloud Security Analyst gab es damals nicht. Man war einfach «die IT» und hat alles gemacht. In diesen frühen Jahren habe ich mir denn auch breite Kenntnisse angeeignet: vom Helpdesk über Systemadministration und Networking bis hin zu Linux Engineering. Kurz gesagt, ich habe dort angepackt, wo es nötig war. Diese breite, praxisnahe Basis prägt meinen Blick auf Technologie bis heute.

Später habe ich eine Führungsrolle in einem stark regulierten FinTech-Umfeld übernommen. Dort kam ich erstmals intensiv mit Security im Hinblick auf Compliance und Governance in Berührung. Themen wie die PCI-DSS-Zertifizierung liessen mich Security-Risiken, Kontrollen und Verantwortlichkeiten neu denken.

Und was hat dich letztlich dazu bewogen, von der klassischen IT zu Cybersecurity zu wechseln?
Vor rund zehn Jahren begann sich in der Branche abzuzeichnen, dass Security zunehmend von den klassischen IT-Operations getrennt wird. Ich bin zunächst bewusst auf der IT-Seite geblieben – einerseits, weil sie mir vertraut war und andererseits, weil das Profil und die Tragweite von Security-Rollen damals noch nicht ganz klar waren. Doch die Entwicklung ging rasant weiter.
Cybersecurity wurde zu einem eigenständigen, vielschichtigen Fachgebiet mit eigenen Methoden, Prozessen, Technologien und Fragestellungen. Es war klar, dass IT-Sicherheit längst nicht mehr nur eine Compliance-Übung oder eine Nebenaufgabe ist, sondern ein zentraler Bereich, der spezialisiertes Know-how verlangt. Bald wurde mir bewusst, dass genau dort der grösste Hebel liegt. Das war der Moment, in dem ich mich entschieden habe, mich voll auf Cybersicherheit zu konzentrieren und sie zu meinem Schwerpunkt zu machen.

Woran erkennt man, dass ein Unternehmen IT-Sicherheit nicht ernst (genug) nimmt?
Ein zentrales Warnsignal ist das Fehlen eines strukturierten und kontinuierlichen Security-Awareness-Programms. Wenn Mitarbeitende die Risiken ihres täglichen Handelns nicht verstehen – sei es beim Umgang mit Zugangsdaten, bei Fehlkonfigurationen oder Social Engineering – bleibt die erste Verteidigungslinie praktisch blind. Ohne ein Bewusstsein für die möglichen Folgen von Security-Fehlern greifen selbst gut durchdachte technische Schutzmassnahmen zu kurz.

Ein weiteres klares Anzeichen ist, wenn IT-Sicherheit nur reaktiv statt vorausschauend angegangen wird. In nicht wenigen Organisationen aller Grössen werden ernsthafte Security-Massnahmen nämlich erst dann umgesetzt, wenn der Schaden bereits da ist. Werden Investitionen, Richtlinien und Prozesse erst nach einem Sicherheitsvorfall angestossen, ist Security nicht Teil der Unternehmensstrategie, sondern bloss eine Reaktion im Krisenmodus.

Wie hat sich die Bedrohungslage verändert? Welche neuen Cyberbedrohungen sind in den letzten zwei Jahren entstanden?
Es ist ein Bedrohungsumfeld entstanden, das schneller, präziser und strategisch deutlich schädlicher ist als je zuvor. Treiber für diese Entwicklung sind vor allem die rasche Verbreitung von KI und die wachsende Professionalität der Cyberkriminellen. Eine der grössten Veränderungen betrifft das Tempo: Malware, Phishing-Kampagnen oder Exploits lassen sich heute in kürzester Zeit entwickeln, testen und weiter verfeinern.

xelon

Für IT-Security-Profis bedeutet das eine stetig wachsende Anzahl von Bedrohungen, die sich oftmals schneller verändern, als klassische Security-Zyklen mithalten können.

Gleichzeitig beobachten wir eine klare Verschiebung hin zu deutlich gezielteren Angriffen. Statt breit gestreuter Massenkampagnen nehmen Bedrohungsakteure zunehmend einzelne Unternehmen, spezifische Systeme oder sogar bestimmte Mitarbeitende ins Visier. Solche Angriffe sind oft mehrstufig angelegt und auf Datenabfluss, langfristige Präsenz im System sowie maximalen Schaden ausgelegt.

Hinzu kommt der starke Anstieg hochautomatisierter Reconnaissance: Cyberangreifende setzen KI ein, um IT-Umgebungen systematisch zu scannen, Schwachstellen zu identifizieren und Angriffe passgenau darauf zuzuschneiden.

Apropos Mitarbeitende: Stimmt es, dass sie oft das schwächste Glied in der IT-Security-Kette sind?
Ich würde nicht sagen, dass Mitarbeitende per se das schwächste Glied sind – aber sie brauchen die richtige Sensibilisierung. Entscheidend ist, dass Sicherheit Teil des Arbeitsalltags wird und nicht einmal pro Jahr als Pflichtübung abgehakt wird. Wenn die Mitarbeitenden verstehen, warum bestimmte Security-Regeln und Vorschriften existieren und wie Angreifende tatsächlich vorgehen, sehen sie IT-Security nicht mehr als lästige Zusatzaufgabe.

Awareness-Trainings wirken am besten, wenn sie praxisnah, verständlich und ruhig auch ein bisschen unterhaltsam sind. Aus einem 50-seitigen PDF, das man widerwillig überfliegt, bleibt kaum etwas hängen. Kurze aber regelmässige Inputs, einfache Beispiele und reale Beispiele, was alles schiefgehen kann, sind deutlich nachhaltiger. Ergänzt durch Phishing-Simulationen oder interaktive Workshops steigt die Aufmerksamkeit spürbar.

Mit dem richtigen Ansatz werden Mitarbeitende so vom vermeintlich «schwächsten Glied» zu einer der stärksten Verteidigungslinien. Denn selbst die modernste Technologie kann nicht verhindern, dass jemand auf einen verdächtigen Link klickt, gezielte Sensibilisierung hingegen schon.

Welche Rolle spielt KI heute in der Cyberabwehr und in der Cyberkriminalität?
KI ist heute auf beiden Seiten der Cybersecurity fest verankert. Sie senkt die Einstiegshürden für Cyberangreifende deutlich. Mit KI lassen sich Malware entwickeln, Phishing-Inhalte generieren, Schwachstellen automatisiert aufspüren und überzeugende Social-Engineering-Nachrichten erstellen und dies oft auch ohne tiefgehende technische Kenntnisse. Dadurch werden Cyberangriffe schneller, günstiger und leichter skalierbar. Zudem setzen professionelle Angreifende KI gezielt ein, um besonders wertvolle Assets zu identifizieren und Angriffe präzise auf die jeweilige IT-Umgebung zuzuschneiden.

Auch auf der Verteidigungsseite ist der Einfluss von KI gross. Moderne Security-Lösungen nutzen Machine Learning, um Verhaltensmuster zu erkennen, Anomalien in Echtzeit aufzudecken und grosse Mengen an Ereignissen aus Endpunkten, Netzwerken und Cloud-Plattformen miteinander zu korrelieren. So können Security-Teams verdächtige Aktivitäten früher erkennen und schneller reagieren. Zudem unterstützt KI bei der Automatisierung von Routineaufgaben, etwa bei der Priorisierung von Alerts, der Klassifizierung von IT-Zwischenfällen oder bei konkreten Handlungsempfehlungen. Das verschafft den IT-Security-Profis mehr Zeit für komplexe und kritische Bedrohungen.

Kurz gesagt: KI verstärkt die Fähigkeiten von Cyberangreifenden und Verteidigenden gleichermassen. Unternehmen, die KI gezielt und verantwortungsvoll einsetzen, verschaffen sich einen klaren Vorteil. Wer darauf verzichtet, läuft Gefahr, in einer zunehmend automatisierten und dynamischen Bedrohungslandschaft den Anschluss zu verlieren.

Kann eine Cloud-Infrastruktur genauso sicher sein wie eine On-Premise-IT-Umgebung?
Wenn sie richtig geplant und umgesetzt wird, ist eine Cloud-Infrastruktur vielfach sicherer als eine On-Premise-Infrastruktur.

Ein wichtiger Grund dafür ist der hohe Reifegrad moderner Cloud-Lösungen. Seriöse Provider investieren massiv in Sicherheit – und zwar deutlich mehr, als es sich die meisten Unternehmen intern leisten können. Dazu gehören unter anderem spezialisierte Security-Mitarbeitende, kontinuierliche Schwachstellenanalysen, Threat Intelligence sowie Monitoring rund um die Uhr.

xelon

Dieses Sicherheitsniveau bildet eine solide Basis, die in vielen On-Premise-Umgebungen so nicht erreicht wird.

Hinzu kommt, dass Cloud-Architekturen klar definierte und standardisierte Sicherheitsmuster vorgeben. Richtig konfiguriert reduziert dies viele menschliche Fehler und Inkonsistenzen, die On-Premise-IT-Infrastrukturen häufig auftreten, weil dort noch mehr manuell aufgebaut und gepflegt wird.

Ein weiterer Vorteil liegt in der Automatisierung. Cloud-Plattformen ermöglichen automatische Korrekturen, unveränderliche Deployments, regelmässige Backups und skalierbares Monitoring. Das führt zu schnellerem Patchen, konsistenteren Konfigurationen und einer deutlich kleineren Angriffsfläche. Zusätzlich bieten Cloud-native Services integrierte Redundanz- und Disaster-Recovery-Optionen, was die Resilienz erheblich erhöht.

Wir beobachten zunehmende Skepsis gegenüber globalen Hyperscalern. Warum werden Cloud-Provider wie Microsoft Azure von Schweizer Unternehmen kritischer gesehen?
Ein zentraler Faktor bei dieser Skepsis ist der US-amerikanische CLOUD Act, der 2018 in Kraft getreten ist. Dieses Gesetz verpflichtet US-Unternehmen, Daten an US-Behörden herauszugeben, selbst wenn diese ausserhalb der USA gespeichert sind. Auch wenn ein amerikanischer Cloud-Hyperscaler Rechenzentren in Europa betreibt, kann er also unter Umständen zur Datenfreigabe gezwungen werden.

Eine stark auf nationale Interessen ausgerichtete Politik und schwer kalkulierbare wirtschaftliche Rahmenbedingungen führen ebenfalls dazu, dass Unternehmen in der Schweiz und in Europa die langfristige Verlässlichkeit US-amerikanischer Cloud-Provider zunehmend hinterfragen. Gerade bei sensiblen Daten stellt sich die Frage, ob man diese in eine globale Cloud migrieren sollte.

Wie können Schweizer Cloud-Anbieter wie Xelon diese Sicherheits-, Compliance- und Souveränitätsbedenken adressieren?
In Europa und besonders in der Schweiz rückt das Thema digitale Souveränität immer stärker in den Fokus. Unternehmen wollen genau wissen, wo ihre Daten liegen, welchen Gesetzen sie unterstehen und welchen Einfluss ausländische Behörden darauf haben können. Geopolitische Entwicklungen haben diese Sensibilität weiter verstärkt.

Bei Xelon werden sämtliche Kundendaten ausschliesslich in ISO-zertifizierten Rechenzentren in der Schweiz gespeichert. Damit unterliegen sie vollständig dem Schweizer Datenschutzrecht, das für seine Stabilität, Klarheit und maximalen Schutz der Privatsphäre bekannt ist.

Da die gesamte Infrastruktur unter Schweizer Gerichtsbarkeit betrieben wird, entfällt auch das Risiko, unter ausländische extraterritoriale Gesetze wie den CLOUD Act zu fallen. Für Unternehmen in regulierten Branchen bedeutet das ein deutlich höheres Mass an Rechtssicherheit.
Zudem behalten Kundinnen und Kunden jederzeit die volle Transparenz darüber, wo ihre Workloads laufen, wie Daten verarbeitet werden und welche rechtlichen Rahmenbedingungen gelten. Gerade bei strengen regulatorischen Vorgaben sind lokale Cloud-Provider oft besser positioniert als globale Hyperscaler, um branchenspezifische Anforderungen zu erfüllen und den Compliance-Aufwand zu reduzieren.

Wem gehören die Daten in einer Schweizer Cloud von Xelon?
Die Daten gehören jederzeit zu hundert Prozent den Kundinnen und Kunden. Sie entscheiden selbst, welche Daten in die Cloud migriert werden, wie sie genutzt werden, wer Zugriff hat und wann sie gelöscht werden. Ohne ausdrückliche Anweisung passiert nichts mit diesen Daten.

Xelon stellt ausschliesslich die sichere Cloud-Infrastruktur und Cloud-Management-Plattform bereit, auf der die Systeme betrieben werden. Wir kümmern uns also um Hardware, Netzwerk, Verfügbarkeit und Schutzmechanismen, doch die Daten selbst bleiben vollständig unter der Kontrolle der Kundinnen und Kunden.

Welche Halb- oder Unwahrheiten rund um Security halten sich besonders hartnäckig? Und welche Fehler siehst du in der Praxis?
Die Annahme, Sicherheit sei ein einmaliges Projekt, ist für mich der grösste Fehler. Viele Unternehmen glauben, nach der Einführung einer Firewall, der Aktivierung von Multi-Faktor-Authentifizierung oder dem Bestehen eines Audits sei das Thema erledigt. In Wirklichkeit ist Security ein kontinuierlicher Prozess, der laufend überwacht, angepasst und weiterentwickelt werden muss.

xelon

Bedrohungen verändern sich, IT-Infrastrukturen wachsen, Mitarbeitende kommen hinzu, und Cyberangreifende finden immer neue Wege, Schwachstellen auszunutzen.

Ein weiteres verbreitetes Missverständnis ist, dass Security-Budgets erst nach einem Vorfall erhöht werden müssen. Dieser reaktive Ansatz ist weit verbreitet, aber teuer. Ein Sicherheitsvorfall kostet fast immer mehr als präventive Massnahmen. Gerade IT-Unternehmen erholen sich nicht selten nie mehr von den Reputationsschäden, die Sicherheitslücken oder Cyberangriffe mit sich bringen.

Diese Denkfehler führen oft zu einem gefährlichen Kreislauf: IT-Sicherheit wird unterschätzt, bis etwas passiert, und erst dann priorisiert. Diesen Kreislauf kann man nur durchbrechen, wenn Cybersecurity als fortlaufende und dynamische Disziplin verstanden wird, die dauerhaft Aufmerksamkeit verdient.

Vielen Dank, dass ihr dieses Interview zum Thema Cybersecurity heruntergeladen habt.

Wir hoffen, es hat euch neue Denkanstösse und praxisnahe Impulse für die Ausrichtung eurer IT-Strategie geliefert. Denn: Wie unser Head of Security Nadir Jabiyev deutlich macht, lassen sich IT und Sicherheit heute nicht mehr getrennt betrachten.

Möchtet auch ihr Sicherheitsrisiken lieber vermeiden als darauf zu reagieren? Fragt ihr euch, wie sicher eure Daten und Systeme in einer Schweizer Cloud wirklich sind? Wollt ihr den Aufwand rund um Compliance und regulatorische Vorgaben reduzieren, ohne Security-Kompromisse machen zu müssen?

Vereinbart jetzt ein unverbindliches und kostenloses Beratungsgespräch mit unserem Security- oder Cloud-Architektur-Team.

Extratipp: Im Xelon Blog findet ihr weitere vertiefende Beiträge zu Cybersecurity sowie zu aktuellen Entwicklungen rund um Cloud und Technologie.

xelon