Hvordan I som virksomhed forsvarer jer mod svindel

5 typer af digital svindel, der vinder frem

Tveægget sværd

'Defeating Fraud - AI as the guardian at the gates of digital business' er titlen på Experians seneste Fraud-rapport. I lande på tværs af Europa, Mellemøsten og Afrika samt regionerne omkring Asien og Stillehavet har vi spurgt over 300 seniorledere i hhv. finans-, tele- og eCommerce-sektoren, hvilke trusler og løsninger de ser, når det gælder digital svindel.

Her er AI et tveægget sværd. Det er kort sagt rapportens konklusion. Kunstig intelligens har nemlig på én gang sænket de tekniske færdigheder, der kræves af digitale svindlere samt øget kompleksiteten i de angreb, der udføres. AI er således ansvarlig for udbredelsen og kompleksiteten i de digitale angreb men samtidig også det mest effektive værn mod svindlerne.

Flere smuthuller, højere professionalisme

Angrebenes kompleksitet kommer bl.a. til udtryk i graden af troværdighed, som digital svindel kan udføres med i dag, mens den voksende udbredelse af digital svindel kan ses som direkte konsekvens af den stigende digitalisering af vores samfund som helhed.

Så hvad kan virksomheder stille op mod angrebenes voksende kompleksitet? Og hvilke typer af digital svindel bør man være ekstra på vagt for?

To centrale spørgsmål, vi tager fat på med denne e-bog. Med afsæt i førnævnte rapport lister vi i prioriteret rækkefølge 5 typer af svindel, der er vundet frem den senere tid. Og så kommer vi med råd til, hvordan I forsvarer jer mod de nye typer af digital svindel.

Rigtig god læselyst.

Syntetisk Identitetssvindel

I mange år var vi i Danmark relativt afskærmet for identitets-vindel. NemID efterfulgt af MitID gjorde det svært for bedragerne at svindle med identitet. Det er det fortsat. Men med AI - MitID eller ej – er det blevet væsentlige nemmere og dermed også mere effektivt at svindle med identitet. Det gælder også den type af svindel kaldet Syntetisk Identitetssvindel. Faktisk var det den type af svindel, der så den mest markante stigning i 2023.

Her er der tale om svindel, hvor bedragerne enten helt eller delvist skaber en falsk identitet med hjælp af data, de har plukket fra forskellige kilder: Navne, fødselsdatoer, adresser, kreditkortoplysninger, telefonnumrene eller sågar såkaldt stemmekloning.

Typisk er hensigten at begå økonomisk svindel såsom at skaffe sig adgang til bankkonti, skaffe kreditkort eller optage lån.

Sådan forsvarer I jer mod Syntetisk Identitetssvindel...

Modsvaret findes grundlæggende i grundigere processer for verifikation af jeres kunder, medarbejdere og samarbejdspartnere. Det kan f.eks. gøres gennem *software*, der monitorerer uregelmæssigheder i jeres kundedata og adfærd. Ligesom *sikkerhedscertifikater*, der minimerer risikoen for stjålne data og *to-faktor-autentificering-løsninger* alt sammen er med til at gøre det svære at begå syntetisk identitetssvindel.

Et konkret råd er, at I gør brug af *biometriske data*.
En teknologi, der aftvinger kunder såvel som potentielle samarbejdspartnere fingeraftryk, ansigtsgenkendelse eller stemmeidentifikation. Ligesom I med fordel kan investere i software, der sikrer jeres side med *Device Intelligence*, der giver indsigter i brugerinfo så som sprogpakker, styresystem, skærmstørrelse etc.

Friendly Fraud

Friendly Fraud ses typisk i eCommerce. Og hensigterne bag er ikke altid onde. Ofte er der tale om et køb, som 'svindleren' ikke kan huske eller genkende, når det dukker op på deres kontoudtog. Svindlen sker, når vedkommende forsøger at kræve pengene retur eller helt stoppe betalingen.

Sådan forsvarer I jer mod Friendly Fraud...

Tydelige beskrivelser af jeres varer er et simpelt men effektivt våben mod Friendly Fraud. Det minimerer risikoen for, at kunden ikke kan huske eller genkende transaktionen. Samme tydelighed bør også gælde alt fra betalingsvilkår over politikker til dokumentation af transaktioner og korrespondancer. På den måde undgås misforståelser, og I står med beviserne, hvis tvivlen alligevel opstår.

Identitetstyveri

Identitetstyveri sker, når bedragerne får adgang til andres personlige oplysninger, som gør det muligt for dem at udgive sig for den pågældende person.

Incitamentet bag identitetstyveri vil ofte være at optage et lån, køb af varer eller tjenester eller phishing. For virksomheder kan identitetstyveriet føre til, at bedragerne får adgang til jeres it-systemer med sabotage eller andre former for it-kriminalitet som følge.

Sådan forsvarer I jer mod identitetstyveri...

Beskyt jeres data. Kort sagt. Det gør I bl.a. gennem stærke adgangskoder, to-faktor godkendelse og regelmæssige opdatering af systemer samt implementering af software, der beskytter mod datakompromittering.

Derudover vil en proaktiv og hurtigreagerende kundesupport være afgørende, når mistanken om identitetstyveri opstår. Mens alle medarbejdere på tværs af virksomheden bør uddannes i, hvordan personlige oplysninger og identitetssikkerhed skal håndteres.

En form for bedrageri, hvor svindlerne tvinger sig adgang til virksomhedens online konti ved hjælp af stjålne legitimationsoplysninger eller teknikker som phishing og malware. Account Takeover vil ofte være resultatet af identitetstyveri og syntetisk identitetstyveri med konsekvenser, der potentielt set er langt mere katastrofale – fra økonomisk tab over skadet omdømme til massive tab af data.

Sådan forsvarer I jer mod account takeover...

Mange af de samme forholdsregler for Identitetstyveri og Syntetisk Identitetstyveri gør sig også gældende her. Det mest effektive værn mod account takeover er i dag to-faktor-autentificering.

Derudover bør der implementeres software, som sikrer jer kontinuerlig overvågning af sikkerhedshændelser og mistænkelig aktivitet. Det vil betyde, at I har større chance for at opdage og reagere prompte på en eventuel indtrængning.

Der bør udføres regelmæssige opdateringer af sikkerhedssystemer og software, der sikrer, at eventuelle smuthuller lukkes.

Og ligesom med identitetstyveri er en grundig uddannelse af medarbejderne på tværs af virksomheden alfa og omega i værnet mod Account Takeover.

60%

Steg 60 pct. i Finans- og telesektoren

36%

Steg med 36 pct. i eCommere-sektoren

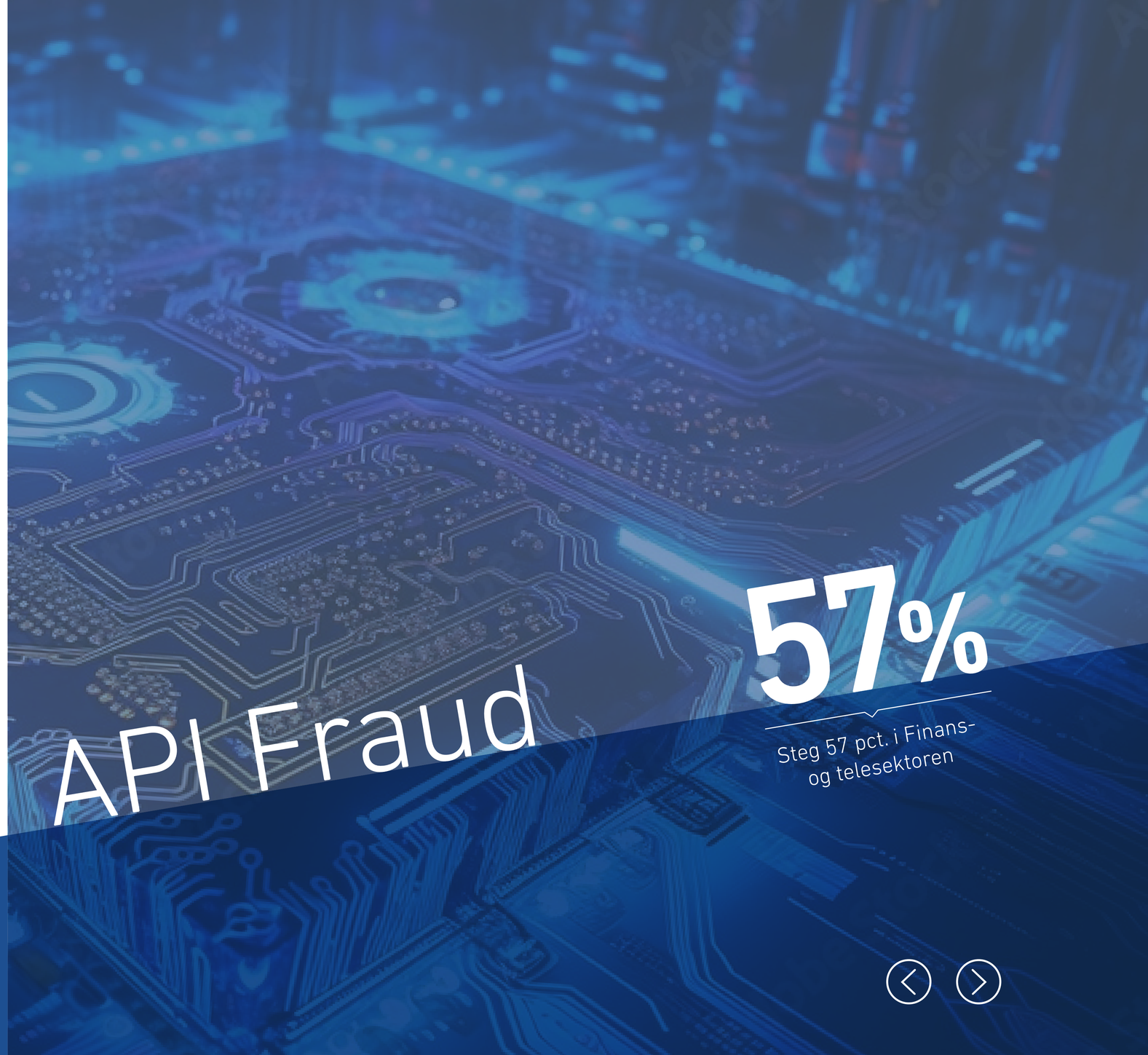
API

Nu bliver det en smule teknisk. API (Application Programming Interface) er stykker af kode, der giver udviklere mulighed for at kommunikere med hele systemer eller databaser. Svindlen (API Fraud) sker, når bedragerne formår at udnytte svagheder eller fejl i jeres API, så de nu kan begå transaktioner, stjæle, ændre eller slette data samt forårsage systemnedbrud eller andre former for skade.

Sådan forsvarer I jer mod API Fraud...

Autentificerings-mekanismer såsom *to-faktor-autentificering* samt implementering af diverse *sikkerhedsprotokoller* er og bliver det bedste våben mod svindel, herunder API Fraud.

Implementer **software**, der overvåger al API-trafik, så I kan identificere mistænkelige mønstre og unormale anmodninger. Og så bør I **regelmæssigt teste og opdatere** API'en med henblik på at lukke potentielle smuthuller.



Afsluttende

Fælles for de fem typer af svindel, vi har beskrevet foroven, er, at de qua teknologier som AI er langt mere komplekse, troværdige og effektive i dag.

GRUNDLÆGGENDE SER VI TRE UDFORDRINGER I FOREBYGGELSEN AF DIGITAL SVINDEL.

1

Evnen til at identificere og opdage, når svindlerne er på besøg i systemerne.

2

Evnen til at skabe effektiv autentificering af kunder, medarbejdere og potentielle samarbejds-partnere.

3

At antallet af løsninger løber løbsk i takt med angrebenes kompleksitet.

Det simple budskab er, at virksomheder i dag er nødsaget til at styrke alle potentielle fronter i værnet mod svindlerne - fra implementering af sikkerhedsprocesser og software til grundig overvågning af vigtige systemer og uddannelse af medarbejdere.

Men det er og bliver som sagt mere kompliceret end som så.

For mens en type af løsninger er optimal til én type af virksomhed, skal andres tænkes ind ift. til andre typer af virksomheder.

Det kan vi hjælpe jer med!

Er I interesseret i at vide mere om, hvilke løsninger, der er optimale at implementere ift. jeres virksomhed og risikoprofil, så tøv ikke med at kontakte os på **experian.dk** eller **70 10 01 07**