

Darkwebovervåking

Oppdag opplysninger på avveie før de blir brukt mot dere

E-postadresser, passord og bedriftsinformasjon kan komme på avveie uten at dere merker det. Etisk Hacker AS overvåker kilder der slike opplysninger deles og omsettes, og varsler om relevante funn. Det gir dere mulighet til å reagere tidligere og redusere risikoen for misbruk.

HVORFOR VIRKSOMHETEN TRENGER DETTE

01

En lekkasje kan bli en vei inn

Et passord fra en ekstern tjeneste kan gi en angriper et forsprang dersom det også brukes på jobb.

Verdi: Oppdag eksponerte innlogginger og få grunnlag for tiltak.

02

Sikkerhet har også en utside

Brannmur og antivirus gir ikke alene oversikt over opplysninger som allerede sirkulerer utenfor egne systemer.

Verdi: Innsikt i eksponering dere ellers kan gå glipp av.

03

Deres navn kan misbrukes

Lignende domener og kopierte nettsider kan brukes for å lure kunder, leverandører og ansatte.

Verdi: Tidligere varsling om forsøk på å utgi seg for dere.

04

Risikoen endrer seg løpende

Nye lekkasjer og svindelforsøk kan dukke opp etter en sikkerhetssjekk. Et enkelt søk er et øyeblikksbilde.

Verdi: Løpende oppfølging av nye funn gjennom abonnementet.

Hva er egentlig dark web

Dark web er en del av nettet som krever særskilt programvare for tilgang. Her finnes blant annet forum og markeds plasser hvor stjålne data deles eller selges. Relevant informasjon kan også dukke opp i andre lekkasjekilder og nettmiljøer som inngår i tjenesten.

Jo tidligere dere kjenner til eksponeringen, desto tidligere kan dere undersøke funnet og begrense mulig skade.

Dette får dere med tjenesten

Overvåking som gir grunnlag for konkrete tiltak

Vi knytter overvåkingen til avtalte domener og virksomhetsopplysninger. Relevante funn varsles slik at dere kan vurdere risikoen og følge opp med IT-ansvarlig eller driftsleverandør.

01 Datalekkasjer og passord på avveie

Søk etter bedriftsopplysninger og eksponerte innloggingsdata i kjente lekkasjer og markeds plasser.

02 Misbruk av virksomhetens identitet

Overvåking av domeneregistreringer og kopierte nettsider som kan brukes til å utgi seg for virksomheten.

03 Trusselinformasjon

Overvåking av relevante forum og diskusjoner på grey og dark web etter informasjon knyttet til virksomheten.

Slik kan et varsel gjøre en forskjell

Eksempel: En ansatts jobbadresse og et passord blir funnet i en datalekkasje fra en ekstern tjeneste. Funnet betyr ikke i seg selv at jobbkontoen er overtatt, men gir grunn til å undersøke eksponeringen.

IT kan undersøke om passordet er gjenbrukt, bytte berørte passord og kontrollere innlogginger. Ved mistanke om kontooveretakelse kan aktive økter avsluttes og hendelsen håndteres videre. Varslet gir et konkret utgangspunkt for handling.

Få oversikt før opplysningene blir misbrukt

Kontakt oss for en kort gjennomgang av domener, varslingsrutiner og abonnement tilpasset virksomheten.

eddie@etiskhacker.no | +47 400 13 483 | etiskhacker.no

Overvåkingen dekker kildene som inngår i tjenesten og kan ikke avdekke alle lekkasjer eller stoppe angrep alene. Omfang, varsling og eventuell bistand ved funn avklares før oppstart.