megatrends

Investire nei megatrend | **documento ad uso del consulente**

Raiffeisen Capital Management

Member of RBI Group

Documento destinato all'informazione degli investitori istituzionali o dei partner distributivi. Ne è vietata la trasmissione alla clientela privata

Per Raiffeisen Capital Management si intende Raiffeisen Kapitalanlage GmbH o, in breve, Raiffeisen KAG. | www.rcm-international.com

Investire nei megatrend
Tema: Cybersecurity

Le valutazioni e i posizionamenti seguenti rappresentano la situazione in un dato momento e possono cambiare in qualsiasi momento e senza preavviso. Non costituiscono alcuna previsione sull'andamento futuro dei mercati finanziari o del fondo Raiffeisen Azionario MegaTrends.

Investire nei megatrend:
I megatrend cambiano il mondo in modo fondamentale e sostenibile. Essi non influenzano solo alcuni settori, ma riguardano tutti i livelli della società e pertanto anche il singolo individuo. Per stare al passo con il futuro, le aziende devono affrontare rapidamente questi sviluppi o, idealmente, anticiparli. Le aziende che ci riescono sono di grande interesse per gli investitori, perché promettono "capacità di futuro" e crescita. Il Raiffeisen Azionario MegaTrends è un fondo azionario globale che investe in questo tipo di società.

La più grande violazione della sicurezza di sempre?
Con le notizie su Donald Trump, la transizione alla Casa Bianca, il coronavirus e i lockdown, molti non si sono probabilmente resi conto di una delle più grandi e gravi violazioni - se non la più grande - di dati e reti di computer globali fino ad oggi. Sono state colpite almeno 18.000 reti di computer, tra cui molte delle più grandi aziende ed enti pubblici negli USA, nel Regno Unito, in Germania e in diversi altri paesi. Il cosiddetto "SolarWinds hack" ironicamente è riuscito ad avere luogo su una scala così massiccia solo perché un gran numero di aziende ed enti pubblici volevano proteggersi proprio da un tale attacco. Gli aggressori hanno infettato proprio il software che avrebbe dovuto garantire la sicurezza di tutte queste reti. Questo è stato poi installato presso gli ingenui clienti. La presunta sentinella è poi diventata "l'apriporta segreto" – e non è stato individuato per almeno nove mesi.

Si prevede un aumento massiccio delle spese per la cyber-sicurezza
Il caso dovrebbe avere ancora enormi conseguenze. Una di queste sembra già essere certa: le spese per la sicurezza informatica aumenteranno un'altra volta in modo massiccio nel 2021. Diverse società di ricerca stimano che il settore crescerà di oltre il 10% all'anno nei prossimi cinque, dieci anni. Per il momento non si intravede alcuna fine, al contrario. Perché qui, naturalmente, stiamo assistendo a un'altra massiccia tendenza: la digitalizzazione di quasi tutti i settori e l'accelerazione del trend del lavoro da casa.

La pandemia ha dato un ulteriore impulso a questi sviluppi. Allo stesso tempo, il rapido aumento della digitalizzazione implica che la criminalità informatica non solo si è diffusa nettamente e nel frattempo si è trasformata in un enorme settore di attività per la criminalità organizzata, ma è anche diventata un campo di battaglia per gli operatori statali e semistatali di tutto il mondo. Il tema della (in)sicurezza informatica riguarda tutti quanti: enti, governi, società e privati. Perché la nostra identità - che ci piaccia o meno - sta diventando

sempre più digitale, almeno a fini amministrativi, di consumo, di viaggio, ecc...

La digitalizzazione ci rende sempre più vulnerabili ai cyber-attacchi

Oltre ai furti e allo spionaggio politico e industriale, attualmente sono in forte aumento soprattutto i ricatti contro società e governi. Gli hacker utilizzano il "ransomware" (software di estorsione) per infettare i computer di altri. Questo fa sì che i dipendenti non abbiano più accesso al loro computer o ai loro file e dati, a meno che non venga pagato un riscatto. Questo riscatto spesso è richiesto in criptovalute, perché questo rende impossibile tracciare il percorso successivo del denaro estorto. Negli ultimi cinque anni, sono state addirittura fondate delle aziende a livello internazionale che utilizzano nuovi metodi di attacco sviluppati in tutto il mondo in cambio di denaro per i clienti, nel settore del ransomware, per esempio, in cambio di una quota del 30% dei ricavi generati. Per questo esiste addirittura già un termine: CaaS ("Crime as a Service", in italiano Crimine come servizio).

Un altro metodo popolare usato dai criminali informatici per ottenere denaro è il "phishing", cioè il furto di identità digitali. Anche il concetto di spyware è simile. Si tratta di un software dannoso che infetta il computer o il cellulare e raccoglie informazioni sull'utente e le sue abitudini. Di solito, questo software spia in sottofondo senza essere rilevato per un lungo periodo di tempo e raccoglie dati o controlla l'attività per provocare azioni dannose che colpiscono il computer dell'utente. I cosiddetti "trojan" sono particolarmente insidiosi. Basandosi sulla famosa leggenda del cavallo di Troia, installano inosservatamente una backdoor attraverso la quale gli aggressori possono poi entrare nei sistemi, rubare o modificare i dati e installare ulteriori software malevoli. L'attacco SolarWinds menzionato all'inizio rientra in questa categoria. Secondo le ultime notizie, due team di hacker, indipendentemente l'uno dall'altro, sono stati in grado di installare delle backdoor.

L'eterna lotta tra scudo e spada

Tra le aziende interessate vi sono, tra l'altro, anche altre società di sicurezza informatica, come FireEye, dove gli hacker hanno anche rubato un arsenale di strumenti di intrusione digitale. Indimenticabile la raccolta di strumenti di hacking dei servizi segreti americani NSA, pubblicata qualche anno fa su Internet e quindi subito entrata nell'arsenale di tutti i gruppi di hacker internazionali. Questo evidenzia anche un grande problema in questo settore, ma che dal punto di vista dell'investitore garantirà una lunga crescita: una lotta eterna tra le spade degli attaccanti e gli scudi dei difensori. I metodi di attacco migliorano continuamente, così come l'hardware a disposizione. Le società specializzate nella difesa contro gli attacchi devono quindi, dal canto loro, sviluppare costantemente metodi di rilevamento e di difesa, crittografia e sistemi di sicurezza. E i loro clienti, volenti o nolenti, devono acquistare continuamente questi sistemi di sicurezza migliori e spendere soldi per la sicurezza informatica. Si stima che intanto i danni economici derivanti dal cyber-crimine superino i mille miliardi di dollari all'anno, il 50% in più rispetto a due anni fa. La necessità per le imprese e le autorità di investire continuamente in sistemi di sicurezza efficaci è relativamente elevata.

Nel Raiffeisen Azionario MegaTrends abbiamo in portafoglio tutta una serie di società di software che offrono protezione contro gli attacchi informatici alle aziende e ai consumatori. Attualmente stiamo investendo in modo concreto nelle seguenti società:

- Cyberark: Privileged Account Security
- Okta: Identity Management
- Sailpoint: Identity and Access Management
- Splunk: Log-, Monitoring and Reporting Plattform
- Trend Micro: Soluzioni complete antivirus
- ZScaler: Cloud Security

Conclusione

Il mercato della cyber-sicurezza crescerà significativamente nel prossimo futuro, anche grazie alla continua digitalizzazione di tutti i settori della vita. Allo stesso tempo, però, non è una strada a senso unico per le aziende che operano in questo campo. Molto si basa naturalmente sulla fiducia, anche e soprattutto in questo settore. Le aziende che non possono (più) giustificare la fiducia dei loro clienti e che con le loro soluzioni non offrono la sicurezza promessa saranno rapidamente sostituite da quelle che lo fanno meglio. Pertanto, anche in questo settore sono necessari un continuo e attento monitoraggio e una buona selezione delle aziende da parte del fund management. Di conseguenza, le posizioni nel fondo possono cambiare in qualsiasi momento. I rischi generalmente associati agli investimenti azionari valgono naturalmente anche per le società che operano nell'ambito della cyber-sicurezza.

Günther Schmitt,
Gestore del Raiffeisen Azionario MegaTrends

Gli investimenti nei fondi sono soggetti a rischi più alti, fino alla perdita del capitale.

Il prospetto pubblicato e lei informazioni chiave per gli investitori (KIID) del Raiffeisen Azionario MegaTrends sono disponibili in lingua tedesca ed in lingua inglese sul sito www.rcm-international.com.

Il Raiffeisen Azionario MegaTrends presenta una volatilità elevata, vale a dire che il valore delle quote può essere esposto anche in tempi brevi ad ampie oscillazioni verso l'alto o il basso, non è qui possibile escludere anche perdite di capitale. !

@ **Contattaci!**
Ci potrà contattare scrivendo a info@rcm.at

Disclaimer - Documento ad uso interno del consulente
Il presente documento ha scopo informativo per clienti professionali e/o consulenti e non è consentita la sua distribuzione a clienti privati. Nonostante l'accuratezza delle ricerche, le indicazioni messe a disposizione hanno scopo puramente informativo, sono basate sullo stato delle conoscenze delle persone incaricate della sua redazione al momento dell'elaborazione e possono essere modificate da Raiffeisen Kapitalanlage GmbH (KAG) in qualunque momento senza ulteriore comunicazione. Si esclude qualunque responsabilità della KAG in merito a queste informazioni o alla presentazione orale basata su di esse, in particolare in riferimento all'attualità, esattezza o completezza delle informazioni o fonti d'informazione a disposizione o al realizzarsi di eventuali previsioni ivi formulate.
In questo documento di consulenza si potrebbe talvolta giungere anche ad una rappresentazione vantaggiosa delle caratteristiche del prodotto. In questo contesto, segnaliamo che il cliente deve essere informato in modo equilibrato relativamente al prodotto. Il profilo di rischio e rendimento dei fondi non è paragonabile a quello di un classico libretto di risparmio. Gli investimenti in fondi sono associati a rischi superiori, comprese le perdite del capitale investito. Informazioni più dettagliate sui prodotti menzionati nel presente documento (prospetto, KID, ecc.) sono disponibili all'indirizzo www.rcm.at

Imagine: iStockphoto.com, data di aggiornamento: 14.01.2021
Raiffeisen Kapitalanlage GmbH, Mooslackengasse 12, A-1190 Vienna

Prima di stampare pensa all'ambiente.